Mục lục

[**Mục tiêu học tập** 2](#_Toc162039172)

[**Bắt đầu với chương trình chứng chỉ** 2](#_Toc162039173)

[**Chào mừng bạn đến với Chứng chỉ an ninh mạng của Google** 2](#_Toc162039174)

[**Tổng quan về Chứng chỉ an ninh mạng của Google** 9](#_Toc162039175)

[**Tổng quan khóa 1** 12](#_Toc162039176)

[**Lộ trình Chứng chỉ An ninh mạng của Google của bạn** 20](#_Toc162039177)

[**Chào mừng đến với tuần 1** 38](#_Toc162039178)

[**Cam kết hoàn thành chương trình** 39](#_Toc162039179)

[**Tài nguyên và lời khuyên hữu ích** 39](#_Toc162039180)

[**Tham gia khảo sát chương trình** 46](#_Toc162039181)

[**Bản khảo sát dành cho người tham gia Chứng chỉ An ninh mạng của Google** 48](#_Toc162039182)

[**Kết nối với các bạn cùng lớp của bạn** 48](#_Toc162039183)

[**Giới thiệu về an ninh mạng** 48](#_Toc162039184)

[**Introduction to cybersecurity** 48](#_Toc162039185)

[**Toni: My path to cybersecurity** 52](#_Toc162039186)

[**Responsibilities of an entry-level cybersecurity analyst** 53](#_Toc162039187)

[**Nikki: A day in the life of a security engineer** 56](#_Toc162039188)

[**Common cybersecurity terminology** 57](#_Toc162039189)

[**Test your knowledge: Introduction to cybersecurity** 60](#_Toc162039190)

[**Kỹ năng cốt lõi dành cho chuyên gia an ninh mạng** 60](#_Toc162039191)

[**Core skills for cybersecurity professionals** 60](#_Toc162039192)

[**Veronica: My path to working in cybersecurity** 63](#_Toc162039193)

[**Transferable and technical cybersecurity skills** 64](#_Toc162039194)

[**Tầm quan trọng của an ninh mạng** 69](#_Toc162039195)

[**Khám phá: Giữ an toàn cho tổ chức** 71](#_Toc162039196)

[**Giá trị của an ninh mạng** 74](#_Toc162039197)

[**Kiểm tra kiến ​​thức của bạn: Kỹ năng cốt lõi dành cho chuyên gia an ninh mạng** 74](#_Toc162039198)

[**Đánh giá: Chào mừng đến với thế giới đầy thú vị của An ninh mạng** 74](#_Toc162039199)

[**Gói lại** 74](#_Toc162039200)

[**Thuật ngữ mô-đun 1** 75](#_Toc162039201)

[**Thử thách mô-đun 1** 76](#_Toc162039202)

Bắt đầu hành trình của bạn vào an ninh mạng! Bạn sẽ khám phá lĩnh vực an ninh mạng và tìm hiểu về trách nhiệm công việc của các chuyên gia an ninh mạng.

# **Mục tiêu học tập**

* Giải thích chương trình chứng chỉ này sẽ giúp người học chuẩn bị như thế nào cho sự nghiệp trong lĩnh vực an ninh
* Xác định lĩnh vực bảo mật
* Khám phá trách nhiệm công việc của một nhà phân tích bảo mật cấp đầu vào
* Nhận biết các kỹ năng và kiến ​​thức cốt lõi cần thiết để trở thành nhà phân tích bảo mật
* Mô tả cách các nhà phân tích bảo mật bảo vệ mạng và thông tin

# **Bắt đầu với chương trình chứng chỉ**

## **Chào mừng bạn đến với Chứng chỉ an ninh mạng của Google**

|  |
| --- |
| Hello and welcome to the Google Career Certificate focused on cybersecurity. I'm so excited that you're here! My name is Toni, and I am a Security Engineering Manager at Google. I'll be your instructor for the first course of this certificate program. By starting this course, you've already taken a big step towards building new skills that will help you in your career. |

Xin chào và chào mừng bạn đến với Chứng chỉ nghề nghiệp của Google (Google Career Certificate) tập trung vào an ninh mạng (cybersecurity). Tôi rất vui vì bạn ở đây! Tên tôi là Toni và tôi là Giám đốc kỹ thuật bảo mật tại Google. Tôi sẽ là người hướng dẫn bạn khóa học đầu tiên của chương trình chứng chỉ này. Khi bắt đầu khóa học này, bạn đã tiến được một bước lớn trong việc xây dựng các kỹ năng mới sẽ giúp ích cho bạn trong sự nghiệp của mình.

|  |
| --- |
| Cybersecurity may seem daunting at first, but you'd be surprised by the different backgrounds many of us have. I worked as an intelligence analyst before I got my first job in the security industry, and I'm excited to be your instructor as you begin your journey into security. |

Ban đầu, an ninh mạng có vẻ khó khăn, nhưng bạn sẽ ngạc nhiên bởi nền tảng kiến ​​thức khác nhau mà nhiều người trong chúng ta có. Tôi đã làm việc với tư cách là nhà phân tích tình báo trước khi có công việc đầu tiên trong ngành bảo mật và tôi rất vui được trở thành người hướng dẫn cho bạn khi bạn bắt đầu hành trình vào lĩnh vực bảo mật.

|  |
| --- |
| The demand for security professionals is growing at an incredible rate. By 2030, the U.S. Bureau of Labor Statistics expects security roles to grow by more than 30%, which is higher than the average growth rate for other occupations. |

Nhu cầu về các chuyên gia bảo mật đang tăng với tốc độ đáng kinh ngạc. Đến năm 2030, Cục Thống kê Lao động Hoa Kỳ kỳ vọng vai trò an ninh sẽ tăng hơn 30%, cao hơn tốc độ tăng trưởng trung bình của các ngành nghề khác.

|  |
| --- |
| Global access to the internet is expanding. Every day, more people and organizations are adopting new digital technologies. Having a diverse community of security professionals with unique backgrounds, perspectives, and experiences is essential for protecting and serving different markets. |

Truy cập toàn cầu vào internet đang mở rộng. Mỗi ngày, ngày càng có nhiều người và tổ chức áp dụng các công nghệ kỹ thuật số mới. Việc có một cộng đồng đa dạng gồm các chuyên gia bảo mật có nền tảng, quan điểm và kinh nghiệm độc đáo là điều cần thiết để bảo vệ và phục vụ các thị trường khác nhau.

|  |
| --- |
| Working in security has allowed me to work with people from all around the world. Working with people who have diverse backgrounds ensures that our teams get to ask lots of questions and come up with more creative solutions. |

Làm việc trong lĩnh vực bảo mật đã cho phép tôi làm việc với mọi người từ khắp nơi trên thế giới. Làm việc với những người có nền tảng đa dạng đảm bảo rằng nhóm của chúng tôi có thể đặt nhiều câu hỏi và đưa ra nhiều giải pháp sáng tạo hơn.

|  |
| --- |
| The main objective in security is to protect organizations and people. This line of work allows you to support and interact with people across the globe. |

Mục tiêu chính của bảo mật là bảo vệ các tổ chức và con người. Công việc này cho phép bạn hỗ trợ và tương tác với mọi người trên toàn cầu.

|  |
| --- |
| There are many openings for entry-level security analysts, and employers are struggling to find enough candidates with the right expertise. This program is designed to give you the knowledge and skills you need to start or advance in the security profession. No matter your current skill level, by the time you finish this certificate program, you'll be prepared to find a security-related job or expand your career in security. |

Có rất nhiều cơ hội dành cho các nhà phân tích bảo mật cấp độ đầu vào và các nhà tuyển dụng đang gặp khó khăn trong việc tìm đủ ứng viên có chuyên môn phù hợp. Chương trình này được thiết kế để cung cấp cho bạn kiến ​​thức và kỹ năng cần thiết để bắt đầu hoặc thăng tiến trong nghề bảo mật. Bất kể trình độ kỹ năng hiện tại của bạn là gì, khi bạn hoàn thành chương trình chứng chỉ này, bạn sẽ sẵn sàng tìm một công việc liên quan đến bảo mật hoặc mở rộng sự nghiệp của mình trong lĩnh vực bảo mật.

|  |
| --- |
| You may be wondering, what do security professionals actually do? Have you ever had to update your password online to include a number or a special symbol? If so, then you're already familiar with basic security measures, like password management. And if you've ever received a notification from a service provider about stolen data or a software hack, then you have first-hand experience with the impact of a security breach. If you've ever asked yourself how organizations safeguard data, then you already have two important traits that are necessary to thrive in this industry: curiosity and excitement. |

Có thể bạn đang thắc mắc, các chuyên gia bảo mật thực sự làm gì? Bạn đã bao giờ phải cập nhật mật khẩu trực tuyến của mình để bao gồm một số hoặc một ký hiệu đặc biệt chưa? Nếu vậy thì bạn đã quen với các biện pháp bảo mật cơ bản, như quản lý mật khẩu. Và nếu bạn đã từng nhận được thông báo từ nhà cung cấp dịch vụ về dữ liệu bị đánh cắp hoặc bị hack phần mềm thì bạn đã có trải nghiệm trực tiếp về tác động của vi phạm bảo mật. Nếu bạn từng tự hỏi các tổ chức bảo vệ dữ liệu như thế nào thì bạn đã có sẵn hai đặc điểm quan trọng cần thiết để phát triển trong ngành này: tính tò mò và sự hào hứng.

|  |
| --- |
| Security analysts help minimize risks to organizations and people. Analysts work to proactively guard against incidents while continuously monitoring systems and networks. And, if an incident does occur, they investigate and report their findings. They are always asking questions and looking for solutions. |

Các nhà phân tích bảo mật giúp giảm thiểu rủi ro cho tổ chức và con người. Các nhà phân tích làm việc để chủ động đề phòng sự cố trong khi liên tục giám sát các hệ thống và mạng. Và nếu một sự cố xảy ra, họ sẽ điều tra và báo cáo những phát hiện của mình. Họ luôn đặt câu hỏi và tìm kiếm giải pháp.

|  |
| --- |
| One of the best things about the security industry is the many paths and career options it exposes you to. Each option involves a unique set of skills and responsibilities. No matter what your background is, you'll probably find that you already have some relevant experience. If you enjoy collaborating with and helping others, solving puzzles, and are motivated by challenges, then this is the career for you. |

Một trong những điều tốt nhất về ngành bảo mật là có nhiều con đường và lựa chọn nghề nghiệp mà nó mang lại cho bạn. Mỗi lựa chọn liên quan đến một bộ kỹ năng và trách nhiệm riêng. Cho dù nền tảng của bạn là gì, có thể bạn sẽ thấy rằng mình đã có một số kinh nghiệm liên quan. Nếu bạn thích hợp tác và giúp đỡ người khác, giải các câu đố và được thúc đẩy bởi các thử thách thì đây là nghề nghiệp dành cho bạn.

|  |
| --- |
| For example, my background as an intelligence analyst had nothing to do with cybersecurity. However, having strong critical thinking skills and communication skills provided a solid foundation for my success when I decided to pursue a career in security. |

Ví dụ, nền tảng của tôi là một nhà phân tích tình báo không liên quan gì đến an ninh mạng. Tuy nhiên, việc có kỹ năng tư duy phản biện mạnh mẽ và kỹ năng giao tiếp đã tạo nền tảng vững chắc cho thành công của tôi khi tôi quyết định theo đuổi nghề bảo vệ.

|  |
| --- |
| If you're not sure what direction you want to take in the security industry, that's okay. This program will give you an overview of many different types of available jobs. It will also let you explore certain specialized skill sets to help you figure out where you want to take your career. |

Nếu bạn không chắc chắn mình muốn đi theo hướng nào trong ngành bảo mật thì cũng không sao. Chương trình này sẽ cung cấp cho bạn cái nhìn tổng quan về nhiều loại công việc hiện có khác nhau. Nó cũng sẽ cho phép bạn khám phá một số bộ kỹ năng chuyên biệt nhất định để giúp bạn tìm ra nơi bạn muốn theo đuổi sự nghiệp của mình.

|  |
| --- |
| The Google Career Certificates are designed by industry professionals with decades of experience here at Google. You'll have a different expert from Google guide you through each course in the certificate. We'll share our knowledge in videos, provide practice opportunities with hands-on activities, and take you through real scenarios that you might encounter on the job. |

Chứng chỉ nghề nghiệp của Google được thiết kế bởi các chuyên gia trong ngành với hàng chục năm kinh nghiệm tại Google. Bạn sẽ được một chuyên gia khác của Google hướng dẫn bạn qua từng khóa học trong chứng chỉ. Chúng tôi sẽ chia sẻ kiến ​​thức của mình qua video, cung cấp cơ hội thực hành bằng các hoạt động thực hành và đưa bạn qua các tình huống thực tế mà bạn có thể gặp phải trong công việc.

|  |
| --- |
| Throughout this program, you'll gain hands-on practice with detecting and responding to attacks, monitoring and protecting networks, investigating incidents, and writing code to automate tasks. |

Trong suốt chương trình này, bạn sẽ được thực hành thực hành cách phát hiện và ứng phó với các cuộc tấn công, giám sát và bảo vệ mạng, điều tra sự cố và viết mã để tự động hóa các tác vụ.

|  |
| --- |
| The program is made up of several courses that are designed to help you land an entry-level job. You'll learn about topics like: core security concepts; security domains; network security; computing basics, including Linux and SQL; along with understanding assets, threats, and vulnerabilities. Our goal is to help you reach your goal of joining the security industry. |

Chương trình này bao gồm một số khóa học được thiết kế để giúp bạn có được một công việc ở trình độ đầu vào. Bạn sẽ tìm hiểu về các chủ đề như: khái niệm bảo mật cốt lõi; miền bảo mật; an ninh mạng; kiến thức cơ bản về điện toán, bao gồm Linux và SQL; cùng với sự hiểu biết về tài sản, mối đe dọa và lỗ hổng. Mục tiêu của chúng tôi là giúp bạn đạt được mục tiêu gia nhập ngành bảo mật.

|  |
| --- |
| You'll learn about incident detection and response, as well as how to use programming languages, like Python, to accomplish common security tasks. You'll also gain valuable job search strategies that will benefit you as you begin to find and apply for jobs in the security profession. |

Bạn sẽ tìm hiểu về cách phát hiện và ứng phó sự cố cũng như cách sử dụng các ngôn ngữ lập trình như Python để hoàn thành các tác vụ bảo mật thông thường. Bạn cũng sẽ đạt được các chiến lược tìm kiếm việc làm có giá trị sẽ mang lại lợi ích cho bạn khi bạn bắt đầu tìm và nộp đơn xin việc trong ngành bảo mật.

|  |
| --- |
| Completing this Google Career Certificate will help you develop skills and learn how to use tools to prepare you for a job in a fast-growing, high-demand field. |

Việc hoàn thành Chứng chỉ nghề nghiệp của Google này sẽ giúp bạn phát triển các kỹ năng và học cách sử dụng các công cụ để chuẩn bị cho bạn làm việc trong lĩnh vực có nhu cầu cao, đang phát triển nhanh.

|  |
| --- |
| The certificate is designed to prepare you for a job in 3-6 months if you work on the certificate part-time. Once you graduate, you can connect with over 200 employers who are interested in hiring Google Career Certificate graduates, like you. Whether you're looking to switch jobs, start a new career, or level up your skills, this Google Career Certificate can open doors to new job opportunities. |

Chứng chỉ này được thiết kế để giúp bạn chuẩn bị cho công việc sau 3-6 tháng nếu bạn làm việc bán thời gian với chứng chỉ đó. Sau khi tốt nghiệp, bạn có thể kết nối với hơn 200 nhà tuyển dụng quan tâm đến việc tuyển dụng những sinh viên tốt nghiệp có Chứng chỉ nghề nghiệp của Google, giống như bạn. Cho dù bạn đang muốn chuyển đổi công việc, bắt đầu một sự nghiệp mới hay nâng cao kỹ năng của mình, Chứng chỉ nghề nghiệp của Google này có thể mở ra những cơ hội việc làm mới.

|  |
| --- |
| You don't need prior experience or knowledge in the security field because this certificate program will begin with the basics. I'll be by your side throughout this first course, making sure that you're learning the foundational knowledge needed to succeed in the field. This program is also flexible. You can complete all of the courses in this certificate on your own terms and at your own pace, online. |

Bạn không cần có kinh nghiệm hoặc kiến ​​thức trước đó trong lĩnh vực bảo mật vì chương trình chứng chỉ này sẽ bắt đầu với những điều cơ bản. Tôi sẽ đồng hành cùng bạn trong suốt khóa học đầu tiên này, đảm bảo rằng bạn đang học những kiến ​​thức nền tảng cần thiết để thành công trong lĩnh vực này. Chương trình này cũng linh hoạt. Bạn có thể hoàn thành trực tuyến tất cả các khóa học trong chứng chỉ này theo điều kiện và tốc độ của riêng bạn.

|  |
| --- |
| We've gathered some amazing instructors to support you on your journey, and they'd like to introduce themselves now: |

Chúng tôi đã tập hợp một số người hướng dẫn tuyệt vời để hỗ trợ bạn trên hành trình của mình và bây giờ họ xin giới thiệu về họ:

|  |
| --- |
| Hi! My name is Ashley, and I'm a Customer Engineering Enablement Lead for Security Operations Sales at Google. I'll take you through security domains, frameworks and controls, as well as common security threats, risks, and vulnerabilities. You'll also be introduced to common tools used by security analysts. I can't wait to get started! |

CHÀO! Tên tôi là Ashley và tôi là Trưởng nhóm hỗ trợ kỹ thuật khách hàng cho hoạt động bán hàng hoạt động bảo mật tại Google. Tôi sẽ hướng dẫn bạn về các miền, khuôn khổ và biện pháp kiểm soát bảo mật cũng như các mối đe dọa, rủi ro và lỗ hổng bảo mật phổ biến. Bạn cũng sẽ được giới thiệu các công cụ phổ biến được các nhà phân tích bảo mật sử dụng. Tôi nóng lòng muốn bắt đầu!

|  |
| --- |
| Hi there! My name is Chris, and I'm the Chief Information Security Officer for Google Fiber. I'm excited to talk to you about the structure of a network, network protocols, common network attacks, and how to secure a network. |

Chào bạn! Tên tôi là Chris và tôi là Giám đốc An ninh Thông tin của Google Fiber. Tôi rất vui được nói chuyện với bạn về cấu trúc của mạng, các giao thức mạng, các cuộc tấn công mạng phổ biến và cách bảo mật mạng.

|  |
| --- |
| Hi there! My name is Kim, and I'm a Technical Program Manager at Google. I will guide you through foundational computing skills that support the work of a security analyst. We'll also learn about operating systems, the Linux command line, and SQL. |

Chào bạn! Tên tôi là Kim và tôi là Giám đốc chương trình kỹ thuật tại Google. Tôi sẽ hướng dẫn bạn các kỹ năng tính toán cơ bản hỗ trợ công việc của một nhà phân tích bảo mật. Chúng ta cũng sẽ tìm hiểu về hệ điều hành, dòng lệnh Linux và SQL.

|  |
| --- |
| Hi! My name is Da'Queshia, and I'm a Security Engineer at Google. Together we'll explore protecting organizational assets through a variety of security controls and develop a deeper understanding of risks and vulnerabilities. |

CHÀO! Tên tôi là Da'Queshia và tôi là Kỹ sư bảo mật tại Google. Cùng nhau, chúng ta sẽ khám phá việc bảo vệ tài sản của tổ chức thông qua nhiều biện pháp kiểm soát bảo mật khác nhau và phát triển sự hiểu biết sâu sắc hơn về các rủi ro và lỗ hổng bảo mật.

|  |
| --- |
| Hi! My name is Dave, and I'm a Principal Security Strategist at Google. In our time together, we'll learn about detecting and responding to security incidents. You'll also have the chance to monitor and analyze network activity using powerful security tools. |

CHÀO! Tên tôi là Dave và tôi là Nhà chiến lược bảo mật chính tại Google. Trong thời gian cùng nhau, chúng ta sẽ tìm hiểu về cách phát hiện và ứng phó với các sự cố bảo mật. Bạn cũng sẽ có cơ hội giám sát và phân tích hoạt động mạng bằng các công cụ bảo mật mạnh mẽ.

|  |
| --- |
| Hello! I'm Angel, and I'm a Security Engineer at Google. We'll explore foundational Python programming concepts to help you automate common security tasks. |

Xin chào! Tôi là Angel và tôi là Kỹ sư bảo mật tại Google. Chúng ta sẽ khám phá các khái niệm lập trình Python cơ bản để giúp bạn tự động hóa các tác vụ bảo mật phổ biến.

|  |
| --- |
| Hello! I'm Dion. I'm a Program Manager at Google. I'm your instructor for the first portion of the final course of the program. There, we'll discuss how to escalate incidents and communicate with stakeholders. |

Xin chào! Tôi là Dion. Tôi là Người quản lý chương trình tại Google. Tôi là người hướng dẫn bạn phần đầu tiên của khóa học cuối cùng của chương trình. Ở đó, chúng ta sẽ thảo luận cách báo cáo sự cố và liên lạc với các bên liên quan.

|  |
| --- |
| And my name is Emily. I'm a Program Manager at Google. I'll guide you through the final portion of the program and share ways that you can engage with the security community and prepare for your upcoming job search. |

Và tên tôi là Emily. Tôi là Người quản lý chương trình tại Google. Tôi sẽ hướng dẫn bạn qua phần cuối cùng của chương trình và chia sẻ những cách mà bạn có thể tương tác với cộng đồng bảo mật và chuẩn bị cho quá trình tìm kiếm việc làm sắp tới của mình.

|  |
| --- |
| And, as you already know, I'll guide you through the first course of this program. This is such a great time to grow your career in the field of security. Sound exciting? Let's get started! |

Và như bạn đã biết, tôi sẽ hướng dẫn bạn khóa học đầu tiên của chương trình này. Đây là thời điểm tuyệt vời để phát triển sự nghiệp của bạn trong lĩnh vực an ninh. Nghe có vẻ thú vị? Bắt đầu nào!

## **Tổng quan về Chứng chỉ an ninh mạng của Google**

|  |
| --- |
| Hello, and welcome to the Google Cybersecurity Certificate! In this program, you will explore the growing field of cybersecurity, learn how cybersecurity is crucial to organizations and the people they serve, and develop relevant skills for a future career in the field. By completing the eight courses in this certificate program, you'll prepare for entry  level jobs in cybersecurity, such as cybersecurity analyst, security analyst, and security operations center (SOC) analyst. No prior experience in cybersecurity is required to complete this program. |

Xin chào và chào mừng bạn đến với Chứng chỉ an ninh mạng của Google! Trong chương trình này, bạn sẽ khám phá lĩnh vực an ninh mạng đang phát triển, tìm hiểu tầm quan trọng của an ninh mạng đối với các tổ chức và những người mà họ phục vụ, đồng thời phát triển các kỹ năng liên quan cho sự nghiệp tương lai trong lĩnh vực này. Bằng cách hoàn thành tám khóa học trong chương trình chứng chỉ này, bạn sẽ chuẩn bị để vào học

các công việc cấp cao trong lĩnh vực an ninh mạng, chẳng hạn như nhà phân tích an ninh mạng, nhà phân tích bảo mật và nhà phân tích trung tâm điều hành bảo mật (SOC). Không cần có kinh nghiệm trước đó về an ninh mạng để hoàn thành chương trình này.

|  |
| --- |
| **Enter a growing field**  Why are skills in cybersecurity in such high demand? The world is undergoing a digital transformation. Every day, global access to the internet is expanding, introducing more devices, more applications, and an even larger amount of data to the World Wide Web. As a result, threats, risks, and vulnerabilities are expanding and causing a significant amount of harm to organizations and people. Cybersecurity professionals are in high demand to help keep organizations, people, and data safe.  Throughout the program, you will have multiple opportunities to develop your cybersecurity knowledge and skills. You will explore concepts and scenarios to learn what an entry-level cybersecurity analyst must know and be able to do to thrive in the cybersecurity profession. |

**Nhập một lĩnh vực đang phát triển**

Tại sao kỹ năng về an ninh mạng lại có nhu cầu cao như vậy? Thế giới đang trải qua quá trình chuyển đổi kỹ thuật số. Mỗi ngày, khả năng truy cập Internet toàn cầu đang mở rộng, giới thiệu nhiều thiết bị hơn, nhiều ứng dụng hơn và lượng dữ liệu thậm chí còn lớn hơn cho World Wide Web. Do đó, các mối đe dọa, rủi ro và lỗ hổng ngày càng mở rộng và gây ra thiệt hại đáng kể cho các tổ chức và con người. Các chuyên gia an ninh mạng đang có nhu cầu cao để giúp giữ an toàn cho các tổ chức, con người và dữ liệu.

Trong suốt chương trình, bạn sẽ có nhiều cơ hội để phát triển kiến ​​thức và kỹ năng về an ninh mạng của mình. Bạn sẽ khám phá các khái niệm và kịch bản để tìm hiểu những điều mà một nhà phân tích an ninh mạng cấp độ đầu vào phải biết và có thể làm để phát triển mạnh trong nghề an ninh mạng.

|  |
| --- |
| **Google Cybersecurity Certificate courses**  The Google Cybersecurity Certificate has eight courses that focus and build upon core concepts and skills related to the daily work of cybersecurity professionals, including foundational cybersecurity models and frameworks that are used to mitigate risk; protecting networks and data; using programming to automate tasks; identifying and responding to security incidents; and communicating and collaborating with stakeholders. Additionally, you will apply what you’ve learned in each course by completing portfolio projects that can be used to showcase your understanding of essential cybersecurity concepts to potential employers. The courses of the program are as follows: |

**Các khóa học Chứng chỉ An ninh mạng của Google**

Chứng chỉ An ninh mạng của Google có tám khóa học tập trung và xây dựng dựa trên các khái niệm và kỹ năng cốt lõi liên quan đến công việc hàng ngày của các chuyên gia an ninh mạng, bao gồm các mô hình và khuôn khổ an ninh mạng cơ bản được dùng để giảm thiểu rủi ro; bảo vệ mạng và dữ liệu; sử dụng lập trình để tự động hóa các nhiệm vụ; xác định và ứng phó với các sự cố an ninh; và giao tiếp và cộng tác với các bên liên quan. Ngoài ra, bạn sẽ áp dụng những gì đã học trong mỗi khóa học bằng cách hoàn thành các dự án danh mục đầu tư có thể được sử dụng để thể hiện sự hiểu biết của bạn về các khái niệm an ninh mạng thiết yếu với các nhà tuyển dụng tiềm năng. Các khóa học của chương trình như sau:

1. [Foundations of Cybersecurity](https://www.coursera.org/learn/foundations-of-cybersecurity/home/module/1).(current course)

2. [Play It Safe: Manage Security Risks](https://www.coursera.org/learn/manage-security-risks)

3. [Connect and Protect: Networks and Network Security](https://www.coursera.org/learn/networks-and-network-security)

4. [Tools of the Trade: Linux and SQL](https://www.coursera.org/learn/linux-and-sql)

5. [Assets, Threats, and Vulnerabilities](https://www.coursera.org/learn/assets-threats-and-vulnerabilities)

6. [Sound the Alarm: Detection and Response](https://www.coursera.org/learn/detection-and-response)

7. [Automate Cybersecurity Tasks with Python](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python)

8. [Put It to Work: Prepare for Cybersecurity Jobs](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs)



|  |
| --- |
| **Benefits for job seekers**  After completing all eight courses, Google Cybersecurity Certificate graduates have access to job search resources, courtesy of Google. You’ll have the opportunity to:   * Build your resume, participate in mock interviews, and receive job search tips through Big Interview, a job-training platform that’s free for program graduates. * Improve your interview technique with Interview Warmup, a tool built by Google with certificate graduates in mind. Access cybersecurity-specific practice questions, transcripts of your responses, and automatic insights that help you grow your skills and confidence. * Access thousands of job postings and free one-on-one career coaching with Career Circle. (You must be eligible to work in the U.S. to join.) * Claim your Google Cybersecurity Certificate badge, and share your achievement on LinkedIn® professional networking services to stand out among other candidates to potential employers. * Prepare for the CompTIA Security+ exam, the industry-leading certification for cybersecurity roles. You’ll earn a dual credential when you complete both the Google Cybersecurity Certificate and the CompTIA Security+ exam.   Congratulations on taking this first step to build your skills for a career in cybersecurity. Enjoy the journey! |

**Lợi ích cho người tìm việc**

Sau khi hoàn thành tất cả tám khóa học, sinh viên tốt nghiệp Chứng chỉ An ninh mạng của Google có quyền truy cập vào các tài nguyên tìm kiếm việc làm do Google cung cấp. Bạn sẽ có cơ hội:

* Xây dựng sơ yếu lý lịch của bạn, tham gia các cuộc phỏng vấn thử và nhận các mẹo tìm việc làm thông qua Big Interview, một nền tảng đào tạo việc làm miễn phí cho sinh viên tốt nghiệp chương trình.
* Cải thiện kỹ thuật phỏng vấn của bạn với Phỏng vấn khởi động, một công cụ do Google xây dựng dành cho những sinh viên tốt nghiệp có chứng chỉ. Truy cập các câu hỏi thực hành dành riêng cho an ninh mạng, bản ghi câu trả lời của bạn và thông tin chi tiết tự động giúp bạn phát triển kỹ năng và sự tự tin của mình.
* Truy cập hàng nghìn tin tuyển dụng và huấn luyện nghề nghiệp trực tiếp miễn phí với Vòng tròn nghề nghiệp. (Bạn phải đủ điều kiện làm việc tại Hoa Kỳ để tham gia.)
* Yêu cầu huy hiệu Chứng chỉ an ninh mạng của Google và chia sẻ thành tích của bạn trên các dịch vụ mạng chuyên nghiệp LinkedIn® để nổi bật giữa các ứng viên khác với các nhà tuyển dụng tiềm năng.
* Chuẩn bị cho kỳ thi CompTIA Security+, chứng chỉ hàng đầu trong ngành về vai trò an ninh mạng. Bạn sẽ nhận được chứng chỉ kép khi hoàn thành cả Chứng chỉ an ninh mạng của Google và bài kiểm tra CompTIA Security+.

Chúc mừng bạn đã thực hiện bước đầu tiên này để xây dựng kỹ năng cho sự nghiệp trong lĩnh vực an ninh mạng. Tận hưởng cuộc hành trình!

## **Tổng quan khóa 1**



|  |
| --- |
| Hello and welcome to **Foundations of Cybersecurity** the first course in the Google Cybersecurity Certificate. You’ve begun an exciting journey!  In this course you will learn the primary job responsibilities and core skills of those who work in the field of cybersecurity. You will explore the eight Certified Information Systems Security Professional (CISSP) security domains various security frameworks and controls as well as a foundational security model called the confidentiality integrity and availability (CIA) triad. You will also be introduced to some common tools used by security analysts that help protect organizations and people alike. |

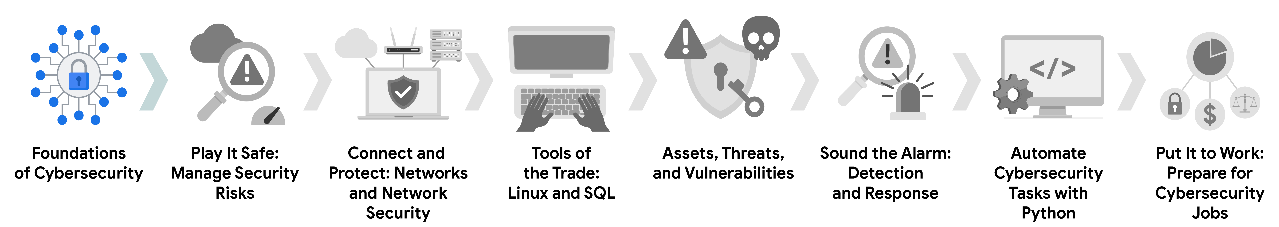
Xin chào và chào mừng bạn đến với Khóa học cơ bản về an ninh mạng, khóa học đầu tiên trong Chứng chỉ an ninh mạng của Google. Bạn đã bắt đầu một cuộc hành trình thú vị!

Trong khóa học này, bạn sẽ tìm hiểu các trách nhiệm công việc chính và kỹ năng cốt lõi của những người làm việc trong lĩnh vực an ninh mạng. Bạn sẽ khám phá tám miền bảo mật của Chuyên gia Bảo mật Hệ thống Thông tin được Chứng nhận (CISSP), các khuôn khổ và biện pháp kiểm soát bảo mật khác nhau cũng như mô hình bảo mật nền tảng được gọi là bộ ba tính toàn vẹn và sẵn sàng bảo mật (CIA). Bạn cũng sẽ được giới thiệu một số công cụ phổ biến được các nhà phân tích bảo mật sử dụng để giúp bảo vệ các tổ chức cũng như con người.

|  |
| --- |
| **Certificate program progress**  The Google Cybersecurity Certificate program has eight courses. Foundations of Cybersecurity is the first course. |

**Tiến độ chương trình chứng chỉ**

Chương trình Chứng chỉ An ninh mạng của Google có tám khóa học. Nền tảng của An ninh mạng là khóa học đầu tiên.



|  |
| --- |
| 1. [Foundations of Cybersecurity](https://www.coursera.org/learn/foundations-of-cybersecurity/home/module/1) - Gain an understanding of network-level vulnerabilities and how to secure networks.  2. [Play It Safe: Manage Security Risks](https://www.coursera.org/learn/manage-security-risks) - Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.  3. [Connect and Protect: Networks and Network Security](https://www.coursera.org/learn/networks-and-network-security) - Gain an understanding of network-level vulnerabilities and how to secure networks.  4. [Tools of the Trade: Linux and SQL](https://www.coursera.org/learn/linux-and-sql) - Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.  5. [Assets, Threats, and Vulnerabilities](https://www.coursera.org/learn/assets-threats-and-vulnerabilities) - Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization’s assets from various threats, risks, and vulnerabilities.  6. [Sound the Alarm: Detection and Response](https://www.coursera.org/learn/detection-and-response) - Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.   1. 7. [Automate Cybersecurity Tasks with Python](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python) - Explore the Python programming language and write code to automate cybersecurity tasks.   8. [Put It to Work: Prepare for Cybersecurity Jobs](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs) - Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search. |

1. [Foundations of Cybersecurity](https://www.coursera.org/learn/foundations-of-cybersecurity/home/module/1) - Hiểu biết về các lỗ hổng ở cấp độ mạng và cách bảo mật mạng.

2. [Play It Safe: Manage Security Risks](https://www.coursera.org/learn/manage-security-risks) - Khám phá các kỹ năng tính toán cơ bản, bao gồm giao tiếp với hệ điều hành Linux thông qua dòng lệnh và truy vấn cơ sở dữ liệu bằng SQL.

3. [Connect and Protect: Networks and Network Security](https://www.coursera.org/learn/networks-and-network-security) - Hiểu biết về các lỗ hổng cấp độ mạng và cách bảo mật mạng.

4. [Tools of the Trade: Linux and SQL](https://www.coursera.org/learn/linux-and-sql) - Khám phá các kỹ năng tính toán cơ bản, bao gồm giao tiếp với hệ điều hành Linux thông qua dòng lệnh và truy vấn cơ sở dữ liệu bằng SQL.

5. [Assets, Threats, and Vulnerabilities](https://www.coursera.org/learn/assets-threats-and-vulnerabilities) - Tìm hiểu về tầm quan trọng của kiểm soát bảo mật và phát triển tư duy của tác nhân đe dọa để bảo vệ và bảo vệ tài sản của tổ chức khỏi các mối đe dọa, rủi ro và lỗ hổng khác nhau.

6. [Sound the Alarm: Detection and Response](https://www.coursera.org/learn/detection-and-response) - Hiểu rõ vòng đời ứng phó sự cố và thực hành sử dụng các công cụ phát hiện và ứng phó sự cố an ninh mạng.

7. [Automate Cybersecurity Tasks with Python](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python) - Khám phá ngôn ngữ lập trình Python và viết mã để tự động hóa các tác vụ an ninh mạng.

8. [Put It to Work: Prepare for Cybersecurity Jobs](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs) - Tìm hiểu về phân loại sự cố, trình báo và cách liên lạc với các bên liên quan. Khóa học này kết thúc chương trình với các mẹo về cách tương tác với cộng đồng an ninh mạng và chuẩn bị cho quá trình tìm kiếm việc làm của bạn.

|  |
| --- |
| **Course 1 content**  Each course of this certificate program is broken into modules. You can complete courses at your own pace, but the module breakdowns are designed to help you finish the entire Google Cybersecurity Certificate in about six months.  What’s to come? Here’s a quick overview of the skills you’ll learn in each module of this course. |

**Nội dung khóa 1**

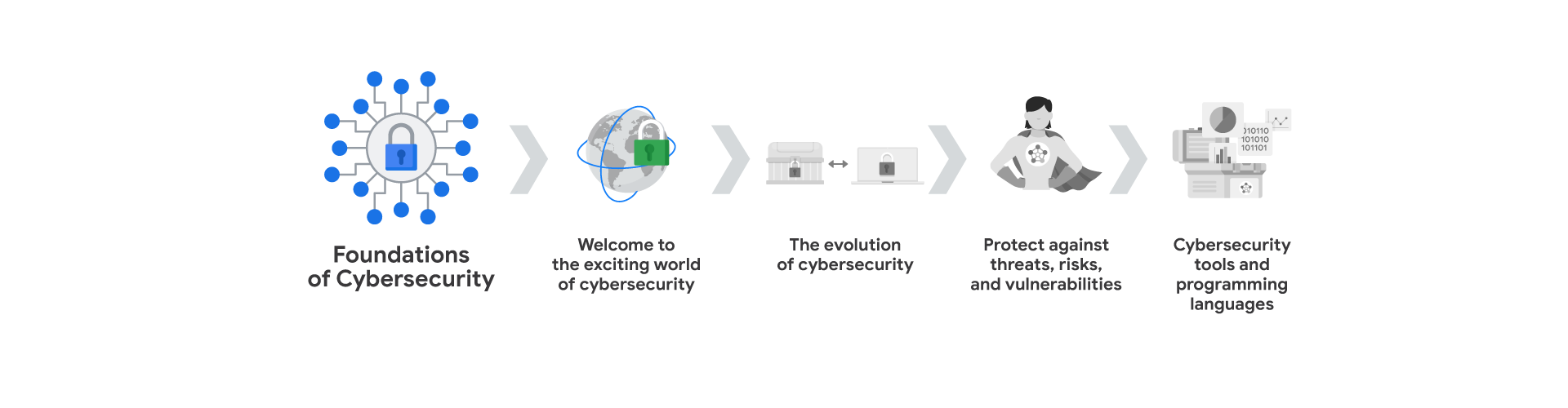
Mỗi khóa học của chương trình chứng chỉ này được chia thành các mô-đun. Bạn có thể hoàn thành các khóa học theo tốc độ của riêng mình nhưng phần phân tích mô-đun được thiết kế để giúp bạn hoàn thành toàn bộ Chứng chỉ an ninh mạng của Google trong khoảng sáu tháng.

Điều gì sẽ đến? Dưới đây là tổng quan nhanh về các kỹ năng bạn sẽ học trong mỗi học phần của khóa học này.

|  |
| --- |
| **Module 1: Welcome to the exciting world of cybersecurity**  Begin your journey into cybersecurity! You'll explore the cybersecurity field, and learn about the job responsibilities of cybersecurity professionals. |

**Mô-đun 1: Chào mừng đến với thế giới thú vị của an ninh mạng**

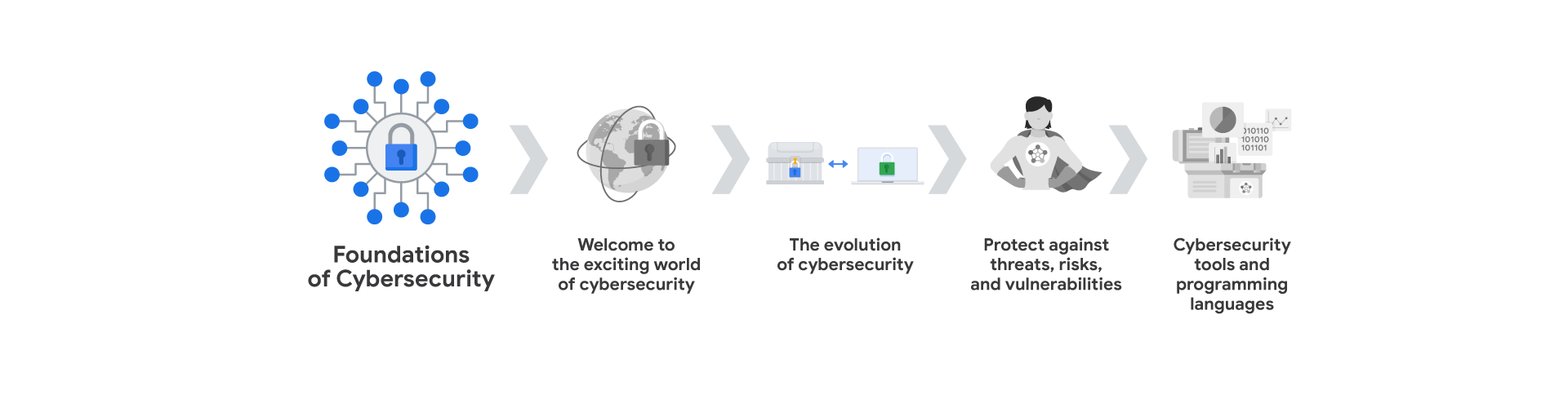
Bắt đầu hành trình của bạn vào an ninh mạng! Bạn sẽ khám phá lĩnh vực an ninh mạng và tìm hiểu về trách nhiệm công việc của các chuyên gia an ninh mạng.



|  |
| --- |
| **Module 2: The evolution of cybersecurity**  You will explore how cybersecurity threats have appeared and evolved alongside the adoption of computers. You will also understand how past and present cyber attacks have influenced the development of the security field. In addition, you'll get an overview of the eight security domains. |

**Mô-đun 2: Sự phát triển của an ninh mạng**

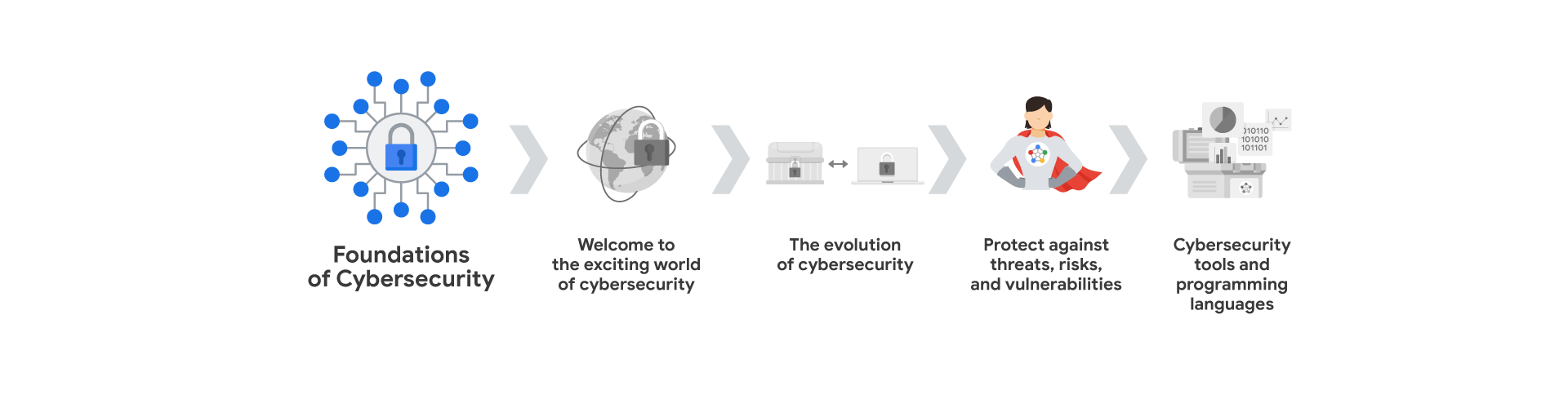
Bạn sẽ khám phá các mối đe dọa an ninh mạng đã xuất hiện và phát triển như thế nào cùng với việc sử dụng máy tính. Bạn cũng sẽ hiểu các cuộc tấn công mạng trong quá khứ và hiện tại đã ảnh hưởng như thế nào đến sự phát triển của lĩnh vực bảo mật. Ngoài ra, bạn sẽ có được cái nhìn tổng quan về tám lĩnh vực bảo mật.



|  |
| --- |
| **Module 3: Protect against threats, risks, and vulnerabilities**  You will learn about security frameworks and controls, which are used to mitigate organizational risk. You'll cover principles of the CIA triad and various National Institute of Standards and Technology (NIST) frameworks. In addition, you'll explore security ethics. |

**Mô-đun 3: Bảo vệ khỏi các mối đe dọa, rủi ro và lỗ hổng**

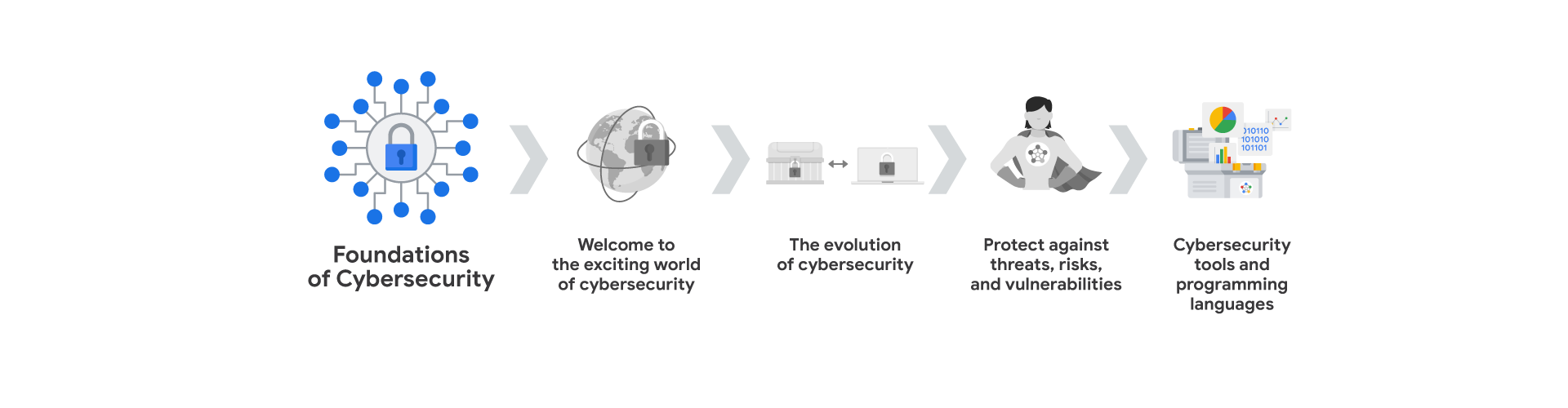
Bạn sẽ tìm hiểu về các khuôn khổ và biện pháp kiểm soát bảo mật được sử dụng để giảm thiểu rủi ro cho tổ chức. Bạn sẽ đề cập đến các nguyên tắc của bộ ba CIA và các khuôn khổ khác nhau của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST). Ngoài ra, bạn sẽ khám phá đạo đức bảo mật.



|  |
| --- |
| Module 4: Cybersecurity tools and programming languages  You’ll discover common tools used by cybersecurity analysts to identify and eliminate risk. You'll learn about security information and event management (SIEM) tools, network protocol analyzers, and programming languages such as Python and SQL. |

**Mô-đun 4: Công cụ an ninh mạng và ngôn ngữ lập trình**

Bạn sẽ khám phá các công cụ phổ biến được các nhà phân tích an ninh mạng sử dụng để xác định và loại bỏ rủi ro. Bạn sẽ tìm hiểu về các công cụ quản lý sự kiện và thông tin bảo mật (SIEM), bộ phân tích giao thức mạng và các ngôn ngữ lập trình như Python và SQL.



|  |
| --- |
| **What to expect**  Each course offers many types of learning opportunities:   * **Videos** led by Google instructors teach new concepts, introduce the use of relevant tools, offer career support, and provide inspirational personal stories. * **Readings** build on the topics discussed in the videos, introduce related concepts, share useful resources, and describe case studies. * **Discussion** **prompts** explore course topics for better understanding and allow you to chat and exchange ideas with other learners in the discussion forums. * **Self-review** **activities** and **labs** give you hands-on practice in applying the skills you are learning and allow you to assess your own work by comparing it to a completed example. * **Interactive plug-ins** encourage you to practice specific tasks and help you integrate knowledge you have gained in the course. * **In-video quizzes** help you check your comprehension as you progress through each video. * **Practice** **quizzes** allow you to check your understanding of key concepts and provide valuable feedback. * **Graded** **quizzes** demonstrate your understanding of the main concepts of a course. You must score 80% or higher on each graded quiz to obtain a certificate, and you can take a graded quiz multiple times to achieve a passing score. |

**Những gì mong đợi**

Mỗi khóa học cung cấp nhiều loại cơ hội học tập:

* **Các video** do người hướng dẫn của Google dẫn dắt dạy các khái niệm mới, giới thiệu cách sử dụng các công cụ có liên quan, cung cấp hỗ trợ nghề nghiệp và cung cấp những câu chuyện cá nhân đầy cảm hứng.\
* **Bài đọc** được xây dựng dựa trên các chủ đề được thảo luận trong video, giới thiệu các khái niệm liên quan, chia sẻ các tài nguyên hữu ích và mô tả các nghiên cứu điển hình.
* **Lời nhắc thảo luận** khám phá các chủ đề khóa học để hiểu rõ hơn và cho phép bạn trò chuyện cũng như trao đổi ý tưởng với những người học khác trong diễn đàn thảo luận.
* **Các hoạt động tự đánh giá và phòng thí nghiệm** giúp bạn thực hành thực hành trong việc áp dụng các kỹ năng bạn đang học và cho phép bạn đánh giá bài làm của chính mình bằng cách so sánh nó với một ví dụ hoàn chỉnh.
* **Các plug-in tương tác** khuyến khích bạn thực hành các nhiệm vụ cụ thể và giúp bạn tích hợp kiến ​​thức bạn đã thu được trong khóa học.
* **Các câu đố trong video** giúp bạn kiểm tra mức độ hiểu của mình khi bạn xem qua từng video.
* **Các câu hỏi thực hành** cho phép bạn kiểm tra sự hiểu biết của mình về các khái niệm chính và cung cấp những phản hồi có giá trị.
* **Các câu hỏi được chấm điểm** thể hiện sự hiểu biết của bạn về các khái niệm chính của khóa học. Bạn phải đạt 80% điểm trở lên trong mỗi bài kiểm tra được xếp loại để nhận được chứng chỉ và bạn có thể làm bài kiểm tra được xếp loại nhiều lần để đạt được điểm đậu.

|  |
| --- |
| **Tips for success**   * It is strongly recommended that you go through the items in each lesson in the order they appear because new information and concepts build on previous knowledge. * Participate in all learning opportunities to gain as much knowledge and experience as possible. * If something is confusing, don’t hesitate to replay a video, review a reading, or repeat a self-review activity. * Use the additional resources that are referenced in this course. They are designed to support your learning. You can find all of these resources in the Resources tab. * When you encounter useful links in this course, bookmark them so you can refer to the information later for study or review. * Understand and follow the Coursera Code of Conduct to ensure that the learning community remains a welcoming, friendly, and supportive place for all members. |

**Lời khuyên để thành công**

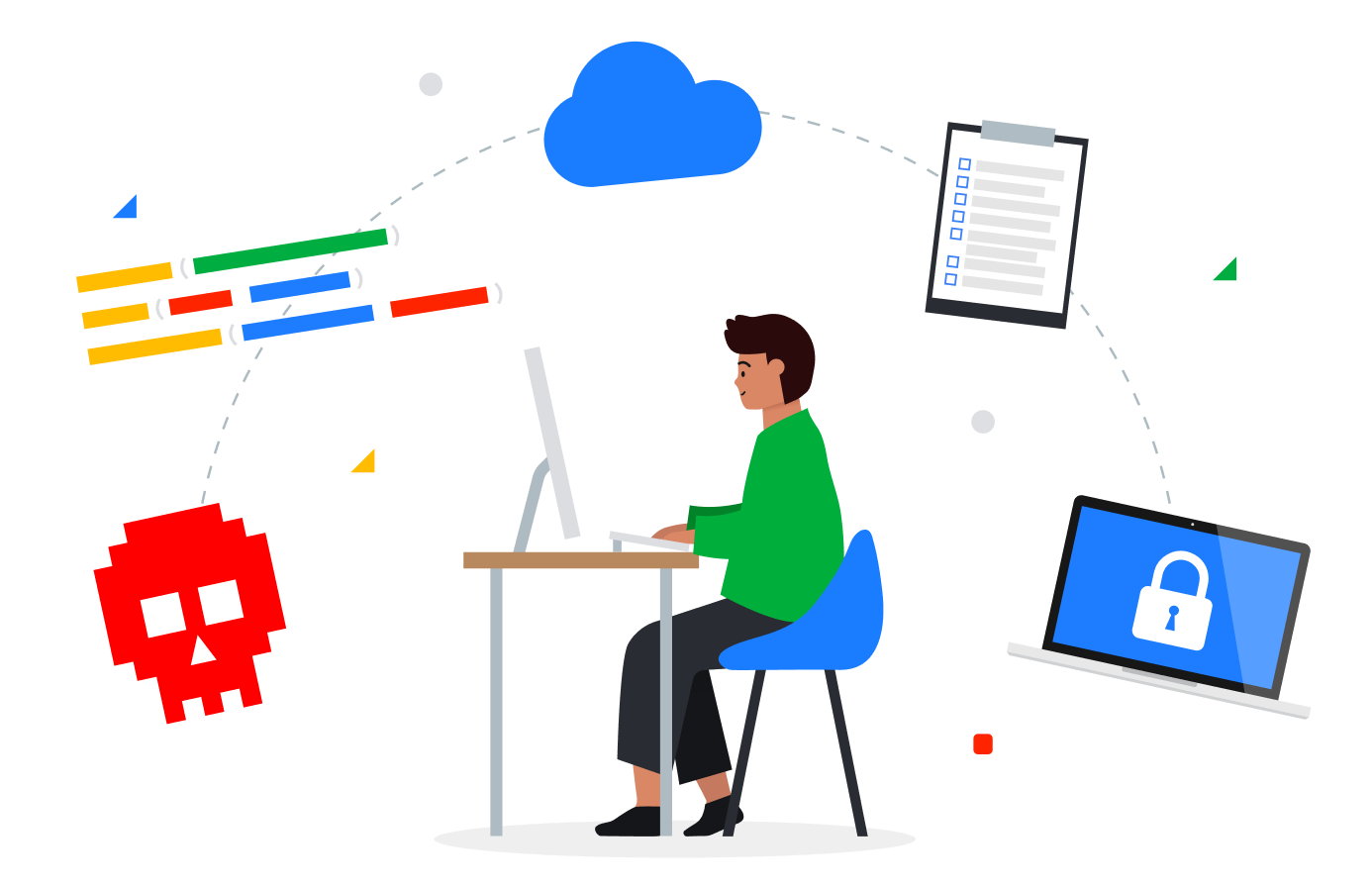
* Chúng tôi đặc biệt khuyên bạn nên xem qua các mục trong mỗi bài học theo thứ tự xuất hiện vì thông tin và khái niệm mới được xây dựng dựa trên kiến ​​thức trước đó.
* Tham gia vào mọi cơ hội học tập để có được càng nhiều kiến ​​thức và kinh nghiệm càng tốt
* Nếu có điều gì đó khó hiểu, đừng ngần ngại phát lại video, xem lại bài đọc hoặc lặp lại hoạt động tự xem xét.
* Sử dụng các tài nguyên bổ sung được tham khảo trong khóa học này. Chúng được thiết kế để hỗ trợ việc học của bạn. Bạn có thể tìm thấy tất cả các tài nguyên này trong tab Tài nguyên.
* Khi bạn gặp những liên kết hữu ích trong khóa học này, hãy đánh dấu chúng để bạn có thể tham khảo thông tin sau này để nghiên cứu hoặc ôn tập.
* Hiểu và tuân theo Quy tắc ứng xử của Coursera để đảm bảo rằng cộng đồng học tập vẫn là nơi thân thiện, thân thiện và hỗ trợ cho tất cả các thành viên.

## **Lộ trình Chứng chỉ An ninh mạng của Google của bạn**

|  |
| --- |
| **Your Google Cybersecurity Certificate roadmap**  Use this guide to review the topics covered, tools used, and skills you will gain in each course. |

**Lộ trình Chứng chỉ An ninh mạng của Google của bạn**

Sử dụng hướng dẫn này để xem lại các chủ đề được đề cập, các công cụ được sử dụng và kỹ năng bạn sẽ đạt được trong mỗi khóa học.



|  |
| --- |
| **Which course?**  For details on topics covered, tools used, and skills you will gain, select the course you’d like to learn more about. |

**Khóa học nào?**

Để biết thông tin chi tiết về các chủ đề được đề cập, các công cụ được sử dụng và kỹ năng bạn sẽ đạt được, hãy chọn khóa học bạn muốn tìm hiểu thêm.

|  |  |
| --- | --- |
| **What tools, solutions, or platforms are included in the curriculum?** | The curriculum includes SIEM tools, playbooks, network and cloud security, network protocol analyzers, and programming languages. |
| **Do I need to take the courses in a certain order?** | We highly recommend completing the courses in the order presented. The content in each course builds on information from previous lessons. |
| **Do I need to have a background in cybersecurity?** | This certificate program is for learners with little to no experience in the cybersecurity field. |
| **How will I develop a professional cybersecurity portfolio?** | Throughout the program, you will have multiple opportunities to apply what you learn in order to create a compelling, relevant portfolio to share during your job search. |

|  |  |
| --- | --- |
| **Những công cụ, giải pháp hoặc nền tảng nào được đưa vào chương trình giảng dạy?** | Chương trình giảng dạy bao gồm các công cụ SIEM, sách hướng dẫn, bảo mật mạng và đám mây, máy phân tích giao thức mạng và ngôn ngữ lập trình. |
| **Tôi có cần tham gia các khóa học theo một thứ tự nhất định không?** | Chúng tôi thực sự khuyên bạn nên hoàn thành các khóa học theo thứ tự được trình bày. Nội dung trong mỗi khóa học được xây dựng dựa trên thông tin từ các bài học trước. |
| **Tôi có cần phải có kiến ​​thức nền tảng về an ninh mạng không?** | Chương trình chứng chỉ này dành cho người học có ít hoặc không có kinh nghiệm trong lĩnh vực an ninh mạng. |
| **Làm cách nào tôi có thể phát triển danh mục đầu tư an ninh mạng chuyên nghiệp?** | Trong suốt chương trình, bạn sẽ có nhiều cơ hội áp dụng những gì mình học được để tạo ra một danh mục đầu tư hấp dẫn, phù hợp để chia sẻ trong quá trình tìm kiếm việc làm của mình. |

#### 1. [Foundations of Cybersecurity](https://www.coursera.org/learn/foundations-of-cybersecurity/home/module/1)



|  |
| --- |
| **In this course, you will:**   * Define the field of security * Recognize core skills and knowledge needed to become a security analyst * Identify how security attacks impact business operations * Identify eight security domains * Define security frameworks and controls |
| **Skill sets:**   * Communicating effectively * Collaborating with others * Identifying threats, risks, and vulnerabilities * Problem-solving |

|  |
| --- |
| **Trong khóa học này, bạn sẽ:**   * Xác định lĩnh vực bảo mật * Nhận biết các kỹ năng và kiến ​​thức cốt lõi cần thiết để trở thành nhà phân tích bảo mật * Xác định các cuộc tấn công bảo mật ảnh hưởng đến hoạt động kinh doanh như thế nào * Xác định tám miền bảo mật * Xác định các khuôn khổ và biện pháp kiểm soát bảo mật |
| **Bộ kỹ năng:**   * Giao tiếp hiệu quả * Cộng tác với người khác * Xác định các mối đe dọa, rủi ro và lỗ hổng * Giải quyết vấn đề |

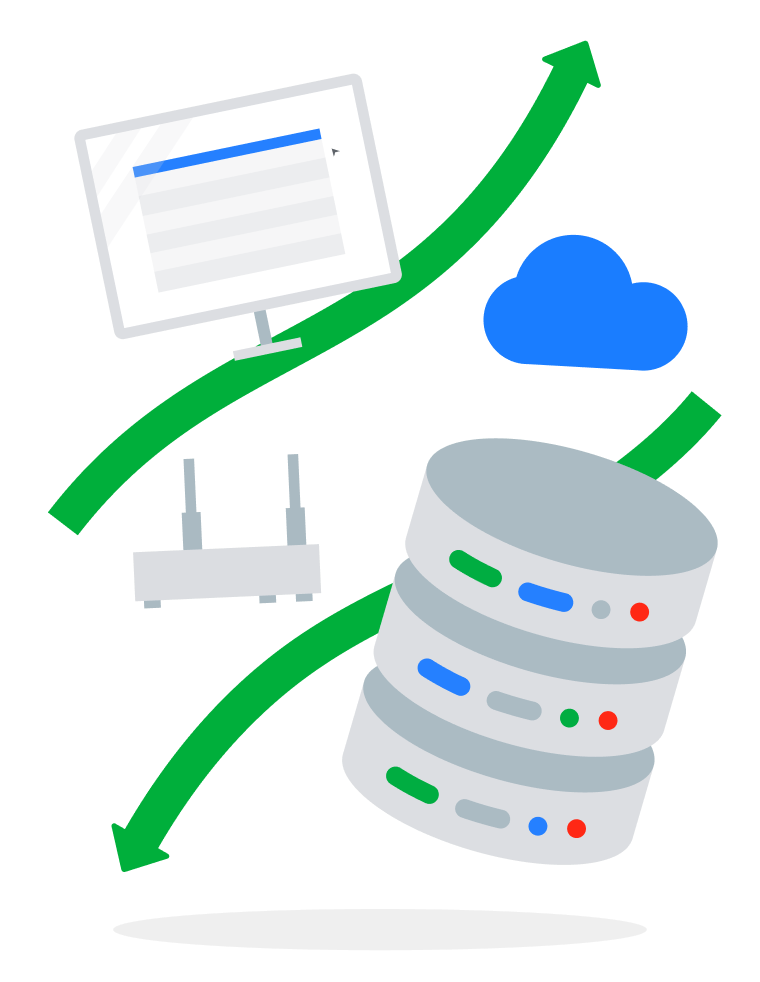
#### 2. [Play It Safe: Manage Security Risks](https://www.coursera.org/learn/manage-security-risks)



|  |
| --- |
| **In this course, you will:**   * Recognize and explain the focus of eight security domains * Identify the steps of risk management * Describe the CIA triad * Identify security principles * Define and describe the purpose of a playbook * Explain how entry-level security analysts use SIEM dashboards |
| **Skill sets:**   * Applying the CIA triad to workplace situations * Analyzing log data * Identifying the phases of an incident response playbook |

|  |
| --- |
| **Trong khóa học này, bạn sẽ:**   * Nhận biết và giải thích trọng tâm của tám lĩnh vực bảo mật * Xác định các bước quản lý rủi ro * Mô tả bộ ba CIA * Xác định các nguyên tắc bảo mật * Xác định và mô tả mục đích của playbook * Giải thích cách các nhà phân tích bảo mật cấp cơ bản sử dụng bảng thông tin SIEM |
| **Bộ kỹ năng:**   * Áp dụng bộ ba CIA vào các tình huống tại nơi làm việc * Phân tích dữ liệu nhật ký * Xác định các giai đoạn của cẩm nang ứng phó sự cố |

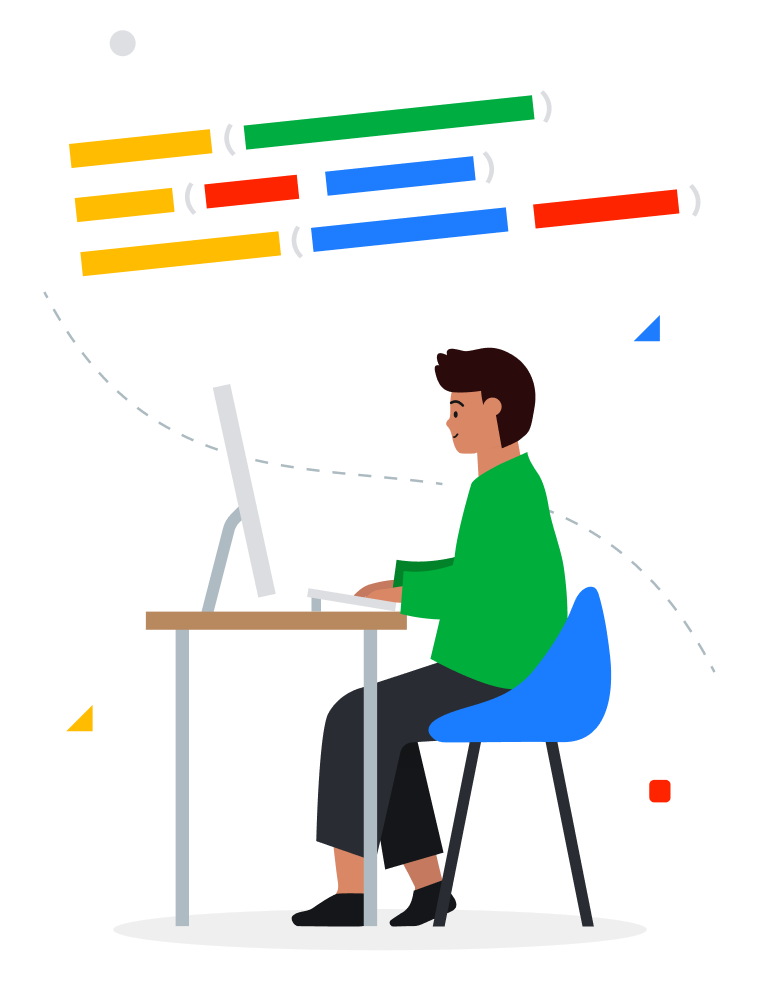
#### 3. [Connect and Protect: Networks and Network Security](https://www.coursera.org/learn/networks-and-network-security)



|  |
| --- |
| **In this course, you will:**   * Define types of networks * Explain how data is sent and received over a network * Recognize common network protocols * Compare and contrast local networks to cloud computing * Explain how to secure a network against intrusion tactics |
| **Skill sets:**   * Configuring a firewall * Recognizing components of computer networks and cloud computing * Analyzing threats * Implementing security hardening |

|  |
| --- |
| **Trong khóa học này, bạn sẽ:**   * Xác định các loại mạng * Giải thích cách gửi và nhận dữ liệu qua mạng * Nhận biết các giao thức mạng phổ biến * So sánh và đối chiếu mạng cục bộ với điện toán đám mây * Giải thích cách bảo mật mạng khỏi các chiến thuật xâm nhập |
| **Bộ kỹ năng:**   * Cấu hình tường lửa * Nhận biết các thành phần của mạng máy tính và điện toán đám mây * Phân tích các mối đe dọa * Thực hiện tăng cường an ninh |

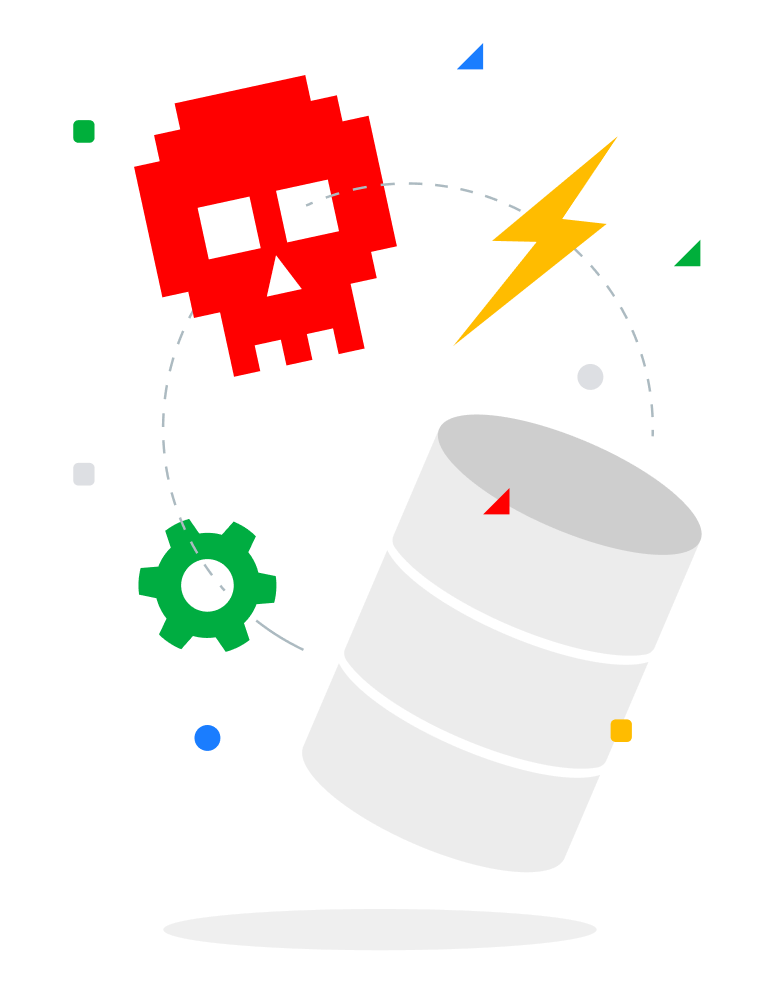
#### 4. [Tools of the Trade: Linux and SQL](https://www.coursera.org/learn/linux-and-sql)



|  |
| --- |
| **In this course, you will:**   * Describe the main functions of an operating system * Explain the relationship between operating systems, applications, and hardware * Compare a graphical user interface to a command line interface * Navigate the file system using Linux commands via the Bash shell * Use SQL to retrieve information from a database |
| **Skill sets:**   * Interacting with both a graphical user interface (GUI) and command line interface (CLI) * Querying a database with SQL * Filtering on a particular word with the Linux command line * Authenticating and authorizing users with the Linux command line |

|  |
| --- |
| **Trong khóa học này, bạn sẽ:**   * Nêu chức năng chính của hệ điều hành * Giải thích mối quan hệ giữa hệ điều hành, ứng dụng và phần cứng * So sánh giao diện người dùng đồ họa với giao diện dòng lệnh * Điều hướng hệ thống tệp bằng lệnh Linux thông qua shell Bash * Sử dụng SQL để lấy thông tin từ cơ sở dữ liệu |
| **Bộ kỹ năng:**   * Tương tác với cả giao diện người dùng đồ họa (GUI) và giao diện dòng lệnh (CLI) * Truy vấn cơ sở dữ liệu bằng SQL * Lọc một từ cụ thể bằng dòng lệnh Linux * Xác thực và ủy quyền người dùng bằng dòng lệnh Linux |

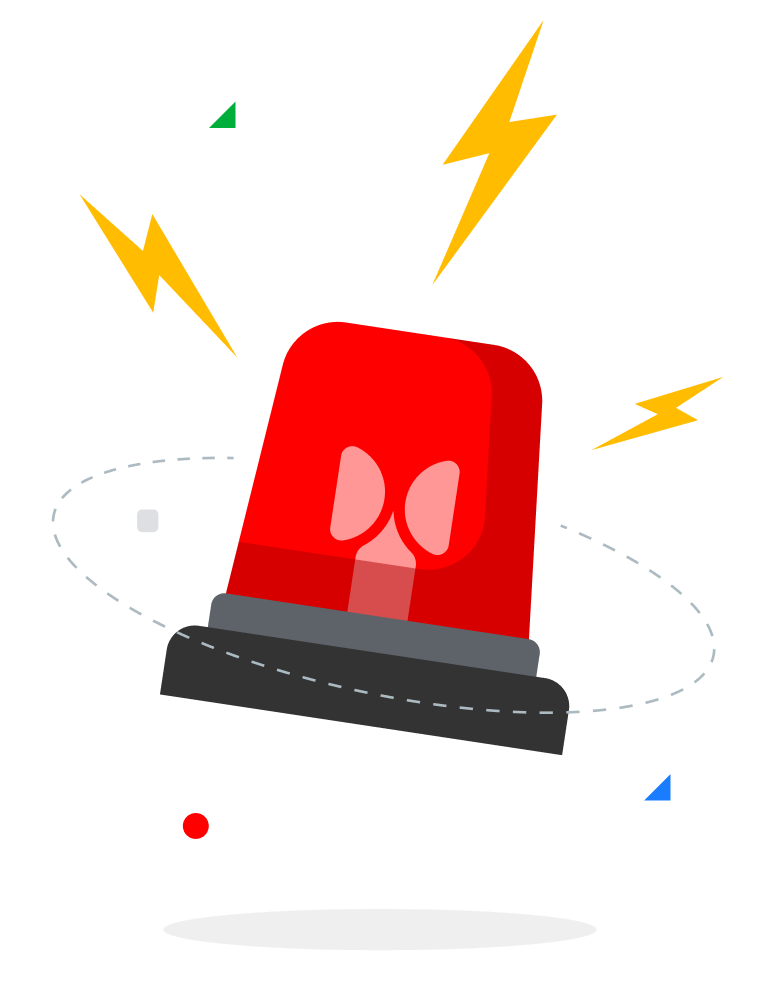
#### 5. [Assets, Threats, and Vulnerabilities](https://www.coursera.org/learn/assets-threats-and-vulnerabilities)



|  |
| --- |
| **In this course, you will:**   * Explain security’s role in mitigating organizational risk * Describe the defense in depth strategy * Explain how vulnerability assessments are used to assess potential risk * Develop an attacker mindset to recognize threats * Discuss the role encryption and hashing play in securing assets * Identify forms of social engineering, malware, and web-based exploits |
| **Skill sets:**   * Classifying assets * Decrypting a message * Searching the CVE database for vulnerable applications * Analyzing attack surfaces * Applying the PASTA threat modeling framework |

|  |
| --- |
| **Trong khóa học này, bạn sẽ:**   * Giải thích vai trò của bảo mật trong việc giảm thiểu rủi ro tổ chức * Mô tả chiến lược phòng thủ theo chiều sâu * Giải thích cách sử dụng đánh giá lỗ hổng để đánh giá rủi ro tiềm ẩn * Phát triển tư duy của kẻ tấn công để nhận ra các mối đe dọa * Thảo luận về vai trò của mã hóa và băm trong việc bảo mật tài sản * Xác định các hình thức tấn công kỹ thuật xã hội, phần mềm độc hại và khai thác dựa trên web |
| **Bộ kỹ năng:**   * Phân loại tài sản * Giải mã tin nhắn * Tìm kiếm cơ sở dữ liệu CVE để tìm các ứng dụng dễ bị tấn công * Phân tích bề mặt tấn công * Áp dụng khung mô hình hóa mối đe dọa PASTA |

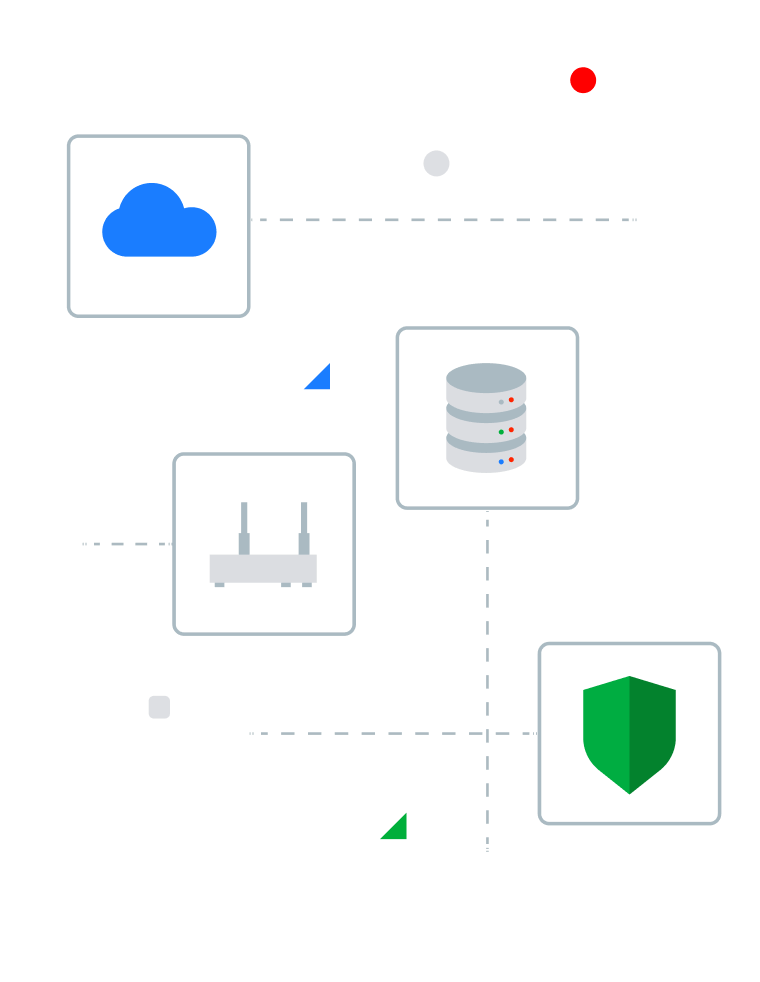
#### 6. [Sound the Alarm: Detection and Response](https://www.coursera.org/learn/detection-and-response)



|  |
| --- |
| **In this course, you will:**   * Explain the lifecycle of an incident * Use packet sniffing tools to capture and view network communications * Perform artifact investigations to analyze and verify security incidents * Identify the steps to contain, eradicate, and recover from an incident * Interpret the basic syntax and components of signatures and logs in IDS and NIDS tools |
| **Skill sets:**   * Capturing, viewing, and analyzing a packet * Investigating a suspicious hash file * Following a playbook * Examining alerts, logs, and rules * Performing queries with SIEM tools |

|  |
| --- |
| **Trong khóa học này, bạn sẽ:**   * Giải thích vòng đời của một sự cố * Sử dụng các công cụ đánh hơi gói để nắm bắt và xem thông tin liên lạc trên mạng * Thực hiện điều tra giả tạo để phân tích và xác minh các sự cố bảo mật * Xác định các bước để ngăn chặn, loại bỏ và phục hồi sau sự cố * Giải thích cú pháp cơ bản và các thành phần của chữ ký và nhật ký trong công cụ IDS và NIDS |
| **Bộ kỹ năng:**   * Chụp, xem và phân tích gói tin * Điều tra một tệp băm đáng ngờ * Theo dõi một vở kịch * Kiểm tra cảnh báo, nhật ký và quy tắc * Thực hiện truy vấn bằng công cụ SIEM |

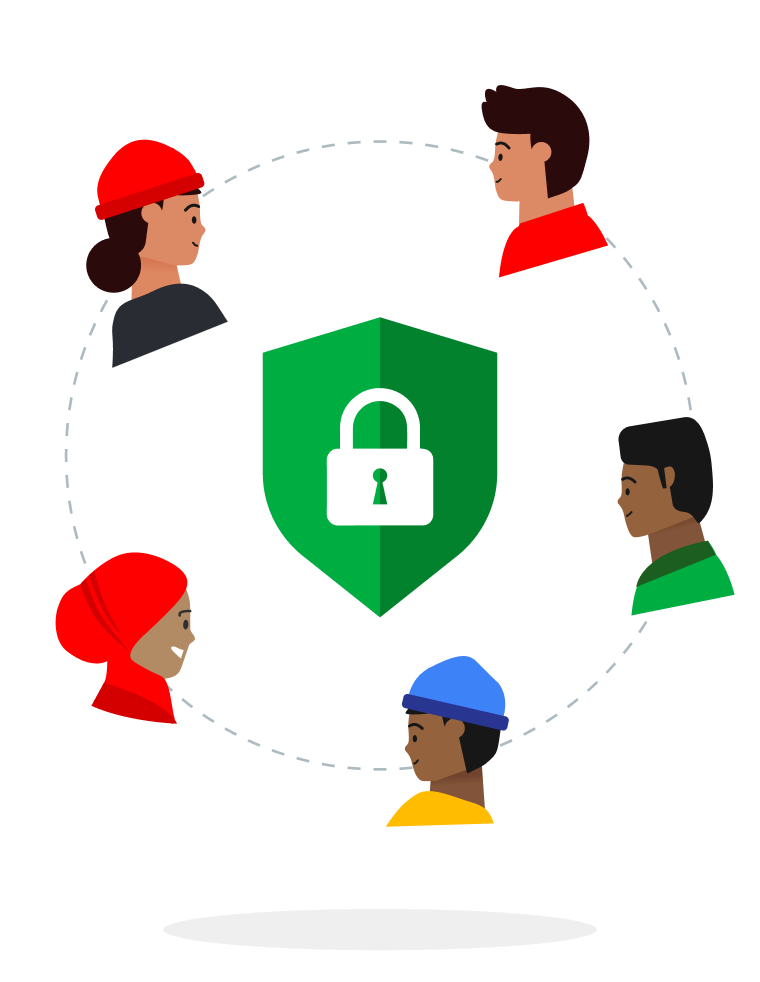
#### 7. [Automate Cybersecurity Tasks with Python](https://www.coursera.org/learn/automate-cybersecurity-tasks-with-python)



|  |
| --- |
| **In this course, you will:**   * Explain how the Python programming language is used in security * Write a simple algorithm * Use regular expressions in Python to extract information from text * Use Python to automate tasks performed by security professionals * Use Python to parse a file |
| **Skill sets:**   * Working with strings and their index values * Applying regular expressions (regex) * Importing and parsing a file * Debugging code |

|  |
| --- |
| **Trong khóa học này, bạn sẽ:**   * Giải thích cách sử dụng ngôn ngữ lập trình Python trong bảo mật * Viết một thuật toán đơn giản * Sử dụng biểu thức chính quy trong Python để trích xuất thông tin từ văn bản * Sử dụng Python để tự động hóa các tác vụ được thực hiện bởi các chuyên gia bảo mật * Sử dụng Python để phân tích một tệp |
| **Bộ kỹ năng:**   * Làm việc với các chuỗi và giá trị chỉ mục của chúng * Áp dụng biểu thức chính quy (regex) * Nhập và phân tích tệp * Mã gỡ lỗi |

#### 8. [Put It to Work: Prepare for Cybersecurity Jobs](https://www.coursera.org/learn/prepare-for-cybersecurity-jobs)



|  |
| --- |
| **In this course, you will:**   * Define stakeholders and describe their security roles * Communicate sensitive information with care and confidentiality * Identify reliable sources within the security community * Determine opportunities to become engaged with the security community * Determine ways to establish and advance a career in security, by engaging with the security community * Find, apply for, and prepare for job interviews |
| **Skill sets:**   * Creating a dashboard * Creating or updating a resume * Using the STAR method for interview questions * Drafting an elevator pitch |

|  |
| --- |
| **Trong khóa học này, bạn sẽ:**   * Xác định các bên liên quan và mô tả vai trò bảo mật của họ * Truyền đạt thông tin nhạy cảm một cách cẩn thận và bảo mật * Xác định các nguồn đáng tin cậy trong cộng đồng bảo mật * Xác định cơ hội tham gia với cộng đồng bảo mật * Xác định các cách để thiết lập và phát triển sự nghiệp trong lĩnh vực bảo mật bằng cách tham gia vào cộng đồng bảo mật * Tìm, nộp đơn và chuẩn bị cho các cuộc phỏng vấn việc làm |
| **Bộ kỹ năng:**   * Tạo bảng điều khiển * Tạo hoặc cập nhật sơ yếu lý lịch * Sử dụng phương pháp STAR cho các câu hỏi phỏng vấn * Soạn thảo một quảng cáo chiêu hàng |

## **Chào mừng đến với tuần 1**

|  |
| --- |
| Hi again! Now that you have some idea of what to expect from the program as a whole, let's discuss more about what you'll learn in this course. |

Chào bạn lần nữa nhé! Bây giờ bạn đã có một số ý tưởng về những gì mong đợi từ toàn bộ chương trình, hãy thảo luận thêm về những gì bạn sẽ học trong khóa học này.

|  |
| --- |
| This course will introduce you to the world of security and how it's used to protect business operations, users, and devices, so you can contribute to the creation of a safer internet for all. |

Khóa học này sẽ giới thiệu cho bạn về thế giới bảo mật và cách nó được sử dụng để bảo vệ hoạt động kinh doanh, người dùng và thiết bị, để bạn có thể góp phần tạo ra một mạng Internet an toàn hơn cho tất cả mọi người.

|  |
| --- |
| In this section, we'll cover foundational security concepts. First, we'll define security. Then, we'll explore common job responsibilities of security analysts. Building on that, we'll cover core skills a security analyst may have. Finally, we'll discuss the value of security for protecting organizations and people. |

Trong phần này, chúng tôi sẽ đề cập đến các khái niệm bảo mật cơ bản. Đầu tiên, chúng ta sẽ định nghĩa bảo mật. Sau đó, chúng ta sẽ khám phá trách nhiệm công việc chung của các nhà phân tích bảo mật. Dựa trên đó, chúng tôi sẽ đề cập đến các kỹ năng cốt lõi mà một nhà phân tích bảo mật có thể có. Cuối cùng, chúng ta sẽ thảo luận về giá trị của bảo mật trong việc bảo vệ các tổ chức và con người.

|  |
| --- |
| Later on, we'll cover eight security domains. Then, we'll cover common security frameworks and controls. Finally, we'll wrap up the course by discussing common tools and programming languages that entry-level security analysts may use. |

Sau này, chúng tôi sẽ đề cập đến tám lĩnh vực bảo mật. Sau đó, chúng tôi sẽ đề cập đến các khuôn khổ và biện pháp kiểm soát bảo mật phổ biến. Cuối cùng, chúng ta sẽ kết thúc khóa học bằng cách thảo luận về các công cụ và ngôn ngữ lập trình phổ biến mà các nhà phân tích bảo mật cấp cơ bản có thể sử dụng.

|  |
| --- |
| Coming up, we'll go over some resources that will allow you to get the most out of this program. I'm really excited for you to start this journey--let's begin! |

Sắp tới, chúng ta sẽ điểm qua một số tài nguyên cho phép bạn tận dụng tối đa chương trình này. Tôi thực sự vui mừng khi bạn bắt đầu cuộc hành trình này--hãy bắt đầu!

## **Cam kết hoàn thành chương trình**

## **Tài nguyên và lời khuyên hữu ích**

|  |
| --- |
| As a learner, you can choose to complete one or multiple courses in this program. However, to obtain the Google Cybersecurity Certificate, you must complete all the courses. This reading describes what is required to obtain a certificate and best practices for you to have a good learning experience on Coursera. |

Là người học, bạn có thể chọn hoàn thành một hoặc nhiều khóa học trong chương trình này. Tuy nhiên, để có được Chứng chỉ an ninh mạng của Google, bạn phải hoàn thành tất cả các khóa học. Bài đọc này mô tả những gì cần thiết để có được chứng chỉ và các phương pháp hay nhất để bạn có trải nghiệm học tập tốt trên Coursera.

|  |
| --- |
| **Course completion to obtain a certificate**  To submit graded assignments and be eligible to receive a Google Cybersecurity Certificate, you must:   * Pay the [course certificate fee](https://www.coursera.support/s/article/209818963-Payments-on-Coursera?language=en_US) or apply and be approved for a Coursera [scholarship](https://www.coursera.support/s/article/209819033-Apply-for-Financial-Aid-or-a-Scholarship?language=en_US). * Pass all graded quizzes in the eight courses with a score of at least 80%. Each graded quiz in a course is part of a cumulative grade for that course. |

**Hoàn thành khóa học để được cấp chứng chỉ**

Để gửi bài tập đã chấm điểm và đủ điều kiện nhận Chứng chỉ an ninh mạng của Google, bạn phải:

* [Trả phí chứng chỉ khóa học](https://www.coursera.support/s/article/209818963-Payments-on-Coursera?language=en_US) hoặc [nộp đơn và được chấp thuận nhận học bổng Coursera](https://www.coursera.support/s/article/209819033-Apply-for-Financial-Aid-or-a-Scholarship?language=en_US).
* Vượt qua tất cả các câu hỏi được chấm điểm trong 8 khóa học với số điểm ít nhất là 80%. Mỗi bài kiểm tra được chấm điểm trong một khóa học là một phần của điểm tích lũy cho khóa học đó.

|  |
| --- |
| **Healthy habits for course completion**  Here is a list of best practices that will help you complete the courses in the program in a timely manner:   * **Plan your time**: Setting regular study times and following them each week can help you make learning a part of your routine. Use a calendar or timetable to create a schedule, and list what you plan to do each day in order to set achievable goals. Find a space that allows you to focus when you watch the videos, review the readings, and complete the activities. * **Work at your own pace**: Everyone learns differently, so this program has been designed to let you work at your own pace. Although your personalized deadlines start when you enroll, feel free to move through the program at the speed that works best for you. There is no penalty for late assignments; to earn your certificate, all you have to do is complete all of the work. You can extend your deadlines at any time by going to **Overview** in the navigation panel and selecting **Switch Sessions**. If you have already missed previous deadlines, select **Reset my deadlines** instead. * **Be curious**: If you find an idea that gets you excited, act on it! Ask questions, search for more details online, explore the links that interest you, and take notes on your discoveries. The steps you take to support your learning along the way will advance your knowledge, create more opportunities in this high-growth field, and help you qualify for jobs. * **Take notes**: Notes will help you remember important information in the future, especially as you’re preparing to enter a new job field. In addition, taking notes is an effective way to make connections between topics and gain a better understanding of those topics. * **Review exemplars**: Exemplars are completed assignments that fully meet an activity's criteria. Many activities in this program have exemplars for you to validate your work or check for errors. Although there are often many ways to complete an assignment, exemplars offer guidance and inspiration about how to complete the activity. * **Build your career identity**: Your career identity is the unique value you bring to the workforce. [Watch this video](https://www.youtube.com/watch?v=_xbT4qMrot4) to learn about the key components of career identity and write your own career identity statement. Discovering and defining your own career identity makes you better equipped to choose a career path that aligns with your strengths, values, and goals and is more effective in your chosen profession. * **Connect with other learners**: If you have a question, chances are, you’re not alone. Reach out in the discussion forum to ask for help from other learners in this program. You can also visit Coursera’s private Google Cybersecurity Community to expand your network, discuss career journeys, and share experiences. Check out the quick start guide. * **Update your profile**: Consider updating your profile on Coursera with your photo, career goals, and more. When other learners find you in the discussion forums, they can click on your name to access your profile and get to know you better. |

**Thói quen lành mạnh khi hoàn thành khóa học**

Dưới đây là danh sách các phương pháp hay nhất sẽ giúp bạn hoàn thành các khóa học trong chương trình một cách kịp thời:

* **Lập kế hoạch thời gian của bạn**: Đặt thời gian học tập thường xuyên và tuân theo chúng mỗi tuần có thể giúp bạn biến việc học trở thành một phần thói quen của mình. Sử dụng lịch hoặc thời gian biểu để tạo lịch trình và liệt kê những việc bạn dự định làm mỗi ngày để đặt ra các mục tiêu có thể đạt được. Tìm một không gian cho phép bạn tập trung khi xem video, xem lại bài đọc và hoàn thành các hoạt động.
* **Làm việc theo tốc độ của riêng bạn**: Mọi người học theo cách khác nhau, vì vậy chương trình này được thiết kế để giúp bạn làm việc theo tốc độ của riêng mình. Mặc dù thời hạn được cá nhân hóa của bạn bắt đầu khi bạn đăng ký, nhưng hãy thoải mái chuyển qua chương trình với tốc độ phù hợp nhất với bạn. Không có hình phạt cho bài tập muộn; để có được chứng chỉ, tất cả những gì bạn phải làm là hoàn thành tất cả công việc. Bạn có thể gia hạn thời hạn của mình bất kỳ lúc nào bằng cách đi tới **Tổng quan** trong bảng điều hướng và chọn **Chuyển đổi phiên**. Nếu bạn đã bỏ lỡ thời hạn trước đó, hãy chọn **Đặt lại thời hạn của tôi**.
* **Hãy tò mò**: Nếu bạn tìm thấy một ý tưởng khiến bạn hứng thú, hãy hành động theo nó! Đặt câu hỏi, tìm kiếm thêm chi tiết trực tuyến, khám phá các liên kết mà bạn quan tâm và ghi chú những khám phá của bạn. Các bước bạn thực hiện để hỗ trợ quá trình học tập của mình sẽ nâng cao kiến ​​thức của bạn, tạo ra nhiều cơ hội hơn trong lĩnh vực có tốc độ tăng trưởng cao này và giúp bạn đủ điều kiện tìm việc làm.\
* **Ghi chú**: Ghi chú sẽ giúp bạn ghi nhớ những thông tin quan trọng trong tương lai, đặc biệt khi bạn đang chuẩn bị bước vào một lĩnh vực công việc mới. Ngoài ra, ghi chép là một cách hiệu quả để tạo sự kết nối giữa các chủ đề và hiểu rõ hơn về các chủ đề đó.
* **Xem lại các mẫu**: Các mẫu là các bài tập đã hoàn thành đáp ứng đầy đủ các tiêu chí của hoạt động. Nhiều hoạt động trong chương trình này có mẫu để bạn xác thực công việc của mình hoặc kiểm tra lỗi. Mặc dù thường có nhiều cách để hoàn thành nhiệm vụ nhưng các ví dụ mẫu sẽ đưa ra hướng dẫn và nguồn cảm hứng về cách hoàn thành hoạt động.
* Xây dựng bản sắc nghề nghiệp của bạn: Bản sắc nghề nghiệp của bạn là giá trị duy nhất mà bạn mang lại cho lực lượng lao động. [Xem video này](https://www.youtube.com/watch?v=_xbT4qMrot4) để tìm hiểu về các thành phần chính của bản sắc nghề nghiệp và viết tuyên bố về bản sắc nghề nghiệp của riêng bạn. Việc khám phá và xác định bản sắc nghề nghiệp của riêng bạn giúp bạn được trang bị tốt hơn để chọn con đường sự nghiệp phù hợp với thế mạnh, giá trị và mục tiêu của mình và hiệu quả hơn trong nghề nghiệp bạn đã chọn.
* **Kết nối với những người học khác**: Nếu bạn có câu hỏi, rất có thể bạn không đơn độc. Hãy liên hệ trong diễn đàn thảo luận để yêu cầu sự giúp đỡ từ những người học khác trong chương trình này. Bạn cũng có thể truy cập trang riêng của Coursera [Cộng đồng an ninh mạng của Google](https://accounts.coursera.org/oauth2/v1/auth?client_id=qWKBUDDMhmx9FERqTKYNHQ&redirect_uri=https%3A%2F%2Fcourseraservices.my.salesforce.com%2Fservices%2Fauthcallback%2FCoursera_Account_SSO&response_type=code&scope=view_profile+view_email_address&state=CAAAAY45vDm-MDAwMDAwMDAwMDAwMDAwAAAA-N65PPBR62xjQJ2BhHGuL1pQFfb6RPeWlxZqLaza44j3T3ZGO2RKpVixB1mR7-mO2zQorqPpMyChUaMStuKnmoeO3RdXl2hdVf-1hRjiWLgNySJV2FQIbURNj0zWy_Mg1iQVmfwIHKz5FukoVh-mhoUOdNq9_amZVklQ9vwoBBjyPS-VC4Xtu-RWp0ItSbjyYnvkHRXpkH-_CmzU1ySqpwZNpxFAMpkIWhNOHckFbS1WEQ25cTaO294Un3R-fiEaxdfGrAql5XZZb76g7Up6KvC_Rww0ibU3LMIBOJ4iY5aHQRrkM-4vhyfRnkFKGfDqxjoxqZatDs_8zEDZn--8BRo%3D) để mở rộng mạng lưới của bạn, thảo luận về hành trình sự nghiệp và chia sẻ kinh nghiệm. [Kiểm tra hướng dẫn nhanh](https://www.coursera.support/s/article/Community-Quick-Start-Guide?language=en_US).
* **Cập nhật hồ sơ của bạn**: Hãy xem xét [cập nhật hồ sơ](https://www.coursera.org/account-profile) của bạn trên Coursera với ảnh của bạn, mục tiêu nghề nghiệp, v.v. Khi những người học khác tìm thấy bạn trong các diễn đàn thảo luận, họ có thể nhấp vào tên của bạn để truy cập hồ sơ của bạn và hiểu rõ hơn về bạn.

|  |
| --- |
| **Documents, spreadsheets, presentations, and labs for course activities**  To complete certain activities in the program, you will need to use digital documents, spreadsheets, presentations, and/or labs. Security professionals use these software tools to collaborate within their teams and organizations. If you need more information about using a particular tool, refer to these resources:   * [Microsoft Word: Help and learning](https://support.microsoft.com/en-us/word): Microsoft Support page for Word * [Google Docs](https://support.google.com/docs/topic/9046002?hl=en&ref_topic=1382883): Help Center page for Google Docs * [Microsoft Excel: Help and learning](https://support.microsoft.com/en-us/excel): Microsoft Support page for Excel * [Google Sheets](https://support.google.com/docs/topic/9054603?hl=en&ref_topic=1382883): Help Center page for Google Sheets * [Microsoft PowerPoint: Help and learning](https://support.microsoft.com/en-us/powerpoint): Microsoft Support page for PowerPoint * [How to use Google Slides](https://support.google.com/docs/answer/2763168?hl=en&co=GENIE.Platform%3DDesktop): Help Center page for Google Slides * [Common problems with labs](https://support.google.com/qwiklabs/answer/9133560?hl=en&ref_topic=9134804): Troubleshooting help for Qwiklabs activities |

**Tài liệu, bảng tính, bài thuyết trình và phòng thí nghiệm cho các hoạt động của khóa học**

Để hoàn thành một số hoạt động nhất định trong chương trình, bạn sẽ cần sử dụng tài liệu kỹ thuật số, bảng tính, bản trình bày và/hoặc phòng thí nghiệm. Các chuyên gia bảo mật sử dụng các công cụ phần mềm này để cộng tác trong nhóm và tổ chức của họ. Nếu bạn cần thêm thông tin về cách sử dụng một công cụ cụ thể, hãy tham khảo các tài nguyên sau:

* [Microsoft Word: Help and learning](https://support.microsoft.com/en-us/word): Trang hỗ trợ của Microsoft dành cho Word
* [Google Docs](https://support.google.com/docs/topic/9046002?hl=en&ref_topic=1382883): Trang Trung tâm trợ giúp dành cho Google Documents
* [Microsoft Excel: Help and learning](https://support.microsoft.com/en-us/excel): Trang hỗ trợ của Microsoft dành cho Excel
* [Google Sheets](https://support.google.com/docs/topic/9054603?hl=en&ref_topic=1382883): Trang Trung tâm trợ giúp dành cho Google Trang tính
* [Microsoft PowerPoint: Help and learning](https://support.microsoft.com/en-us/powerpoint): Trang hỗ trợ của Microsoft dành cho PowerPoint
* [How to use Google Slides](https://support.google.com/docs/answer/2763168?hl=en&co=GENIE.Platform%3DDesktop): Trang Trung tâm trợ giúp dành cho Google Trang trình bày
* [Common problems with labs](https://support.google.com/qwiklabs/answer/9133560?hl=en&ref_topic=9134804): Trợ giúp khắc phục sự cố cho các hoạt động Qwiklabs

|  |
| --- |
| **Module, course, and certificate glossaries**  This program covers a lot of terms and concepts, some of which you may already know and some of which may be unfamiliar to you. To review terms and help you prepare for graded quizzes, refer to the following glossaries:   * **Module glossaries**: At the end of each module’s content, you can review a glossary of terms from that module. Each module’s glossary builds upon the terms from the previous modules in that course. The module glossaries are not downloadable; however, all of the terms and definitions are included in the course and certificate glossaries, which are downloadable. * **Certificate glossary**: The certificate glossary includes all of the terms in the entire certificate program and is a helpful resource that you can reference throughout the program or at any time in the future. * **Course glossaries**: At the end of each course, you can access and download a glossary that covers all of the terms in that course.   You can access and download the certificate glossaries and save them on your computer. You can always find the course and certificate glossaries through the course’s [Resources](https://www.coursera.org/learn/foundations-of-cybersecurity/resources/L1aML) section. To access the **Cybersecurity Certificate glossary**, click the link below and select Use Template.   * [Cybersecurity Certificate glossary](https://docs.google.com/document/d/1Feb8pHRY-blnpaLOohds2esd6IWdCIp-ikG7G_omSj4/template/preview?resourcekey=0-YHcAISkCiqGDq5KwO6yNeQ)   OR   * If you don’t have a Google account, you can download the glossary directly from the attachment below. |

**Bảng thuật ngữ mô-đun, khóa học và chứng chỉ**

Chương trình này bao gồm rất nhiều thuật ngữ và khái niệm, một số trong đó bạn có thể đã biết và một số có thể xa lạ với bạn. Để xem lại các thuật ngữ và giúp bạn chuẩn bị cho các bài kiểm tra được chấm điểm, hãy tham khảo các bảng thuật ngữ sau:

* **Bảng chú giải thuật ngữ của mô-đun**: Ở cuối nội dung của mỗi mô-đun, bạn có thể xem lại bảng chú giải thuật ngữ của mô-đun đó. Bảng thuật ngữ của mỗi mô-đun được xây dựng dựa trên các thuật ngữ từ các mô-đun trước đó trong khóa học đó. Bảng thuật ngữ mô-đun không thể tải xuống được; tuy nhiên, tất cả các thuật ngữ và định nghĩa đều có trong bảng thuật ngữ khóa học và chứng chỉ, có thể tải xuống được.
* **Bảng chú giải thuật ngữ chứng chỉ**: Bảng chú giải thuật ngữ chứng chỉ bao gồm tất cả các thuật ngữ trong toàn bộ chương trình chứng chỉ và là nguồn tài nguyên hữu ích mà bạn có thể tham khảo trong suốt chương trình hoặc bất kỳ lúc nào trong tương lai.
* **Bảng thuật ngữ khóa học**: Vào cuối mỗi khóa học, bạn có thể truy cập và tải xuống bảng chú giải thuật ngữ bao gồm tất cả các thuật ngữ trong khóa học đó.

Bạn có thể truy cập và tải xuống bảng chú giải chứng chỉ và lưu chúng trên máy tính của mình. Bạn luôn có thể tìm thấy bảng thuật ngữ khóa học và chứng chỉ thông qua phần [Tài nguyên](https://www.coursera.org/learn/foundations-of-cybersecurity/resources/L1aML) của khóa học. Để truy cập bảng chú giải Chứng chỉ An ninh mạng, hãy nhấp vào liên kết bên dưới và chọn Sử dụng Mẫu.

• [Thuật ngữ chứng chỉ an ninh mạng](https://docs.google.com/document/d/1Feb8pHRY-blnpaLOohds2esd6IWdCIp-ikG7G_omSj4/template/preview?resourcekey=0-YHcAISkCiqGDq5KwO6yNeQ)

HOẶC

• Nếu chưa có tài khoản Google, bạn có thể tải xuống bảng thuật ngữ trực tiếp từ tệp đính kèm bên dưới.

|  |
| --- |
| **Course feedback**  Providing feedback on videos, readings, and other materials is easy. With the resource open in your browser, you can find the thumbs-up and thumbs-down symbols.   * Click **thumbs-up** for materials you find helpful. * Click **thumbs-down** for materials that you do not find helpful.   If you want to flag a specific issue with an item, click the flag icon, select a category, and enter an explanation in the text box. This feedback goes back to the course development team and isn’t visible to other learners. All feedback received helps to create even better certificate programs in the future.  For technical help, visit the [Learner Help Center](https://learner.coursera.help/hc/en-us). |

**Phản hồi khóa học**

Việc cung cấp phản hồi về video, bài đọc và các tài liệu khác thật dễ dàng. Khi tài nguyên mở trong trình duyệt của bạn, bạn có thể tìm thấy các biểu tượng không thích và không thích.

* + Hãy bấm nút thích để xem những tài liệu bạn thấy hữu ích.
  + Hãy bấm nút không thích đối với những tài liệu mà bạn thấy không hữu ích.

Nếu bạn muốn gắn cờ một vấn đề cụ thể cho một mục, hãy nhấp vào biểu tượng lá cờ, chọn một danh mục và nhập lời giải thích vào hộp văn bản. Phản hồi này sẽ được chuyển lại cho nhóm phát triển khóa học và những người học khác sẽ không nhìn thấy được. Tất cả phản hồi nhận được sẽ giúp tạo ra các chương trình chứng chỉ tốt hơn nữa trong tương lai.

Để được trợ giúp kỹ thuật, hãy truy cập [Trung tâm trợ giúp người học](https://learner.coursera.help/hc/en-us).

## **Tham gia khảo sát chương trình**

|  |
| --- |
| **Participate in program surveys**  During this certificate program, you will be asked to complete a few short surveys. These are part of a research study being conducted to understand how effectively the certificate meets your career training needs. Keep reading for a summary of what each survey will cover.  Your survey participation is optional but extremely helpful in making this program as effective as possible. All data is kept confidential and is aggregated for review in accordance with [Coursera’s privacy policy](https://www.coursera.org/about/privacy). Your name is separated from your data when it is stored.  There are no right or wrong answers. Your responses or personal data:   * Won’t affect your program experience, scores, or ability to receive a certificate or job offer * Won’t be shared outside of our research team unless you give permission to share your contact information with hiring partners   Thanks for your consideration and time! |

**Tham gia khảo sát chương trình**

Trong chương trình chứng chỉ này, bạn sẽ được yêu cầu hoàn thành một số khảo sát ngắn. Đây là một phần của nghiên cứu đang được thực hiện để hiểu mức độ hiệu quả của chứng chỉ đáp ứng nhu cầu đào tạo nghề nghiệp của bạn. Hãy tiếp tục đọc để biết bản tóm tắt về những nội dung mà mỗi cuộc khảo sát sẽ đề cập.

Việc tham gia khảo sát của bạn là tùy chọn nhưng cực kỳ hữu ích trong việc làm cho chương trình này hiệu quả nhất có thể. Tất cả dữ liệu được giữ bí mật và được tổng hợp để xem xét theo [chính sách quyền riêng tư của Coursera](https://www.coursera.org/about/privacy). Tên của bạn được tách khỏi dữ liệu của bạn khi nó được lưu trữ.

Không có câu trả lời đúng hay sai. Phản hồi hoặc dữ liệu cá nhân của bạn:

• Sẽ không ảnh hưởng đến trải nghiệm chương trình, điểm số hoặc khả năng nhận được chứng chỉ hoặc lời mời làm việc của bạn

• Sẽ không được chia sẻ ra bên ngoài nhóm nghiên cứu của chúng tôi trừ khi bạn cho phép chia sẻ thông tin liên hệ của mình với các đối tác tuyển dụng

Cảm ơn sự quan tâm và thời gian của bạn!

|  |
| --- |
| **Entry survey**  First, you will have an opportunity to answer a brief survey to help researchers understand why you enrolled in this certificate program. If you don’t fill out the survey now, you will receive an invitation to fill it out after completing your first video or activity.  The survey asks about your experiences leading up to this program and the goals you hope to achieve. This is critical information to ensure your needs as a learner are met and that this program will continue to be offered in the future. |

**Khảo sát đầu vào**

Đầu tiên, bạn sẽ có cơ hội trả lời một cuộc khảo sát ngắn gọn để giúp các nhà nghiên cứu hiểu lý do tại sao bạn đăng ký tham gia chương trình chứng chỉ này. Nếu không điền vào bản khảo sát ngay bây giờ, bạn sẽ nhận được lời mời điền vào bản khảo sát sau khi hoàn thành video hoặc hoạt động đầu tiên của mình.

Cuộc khảo sát hỏi về trải nghiệm của bạn khi tham gia chương trình này và những mục tiêu bạn hy vọng đạt được. Đây là thông tin quan trọng để đảm bảo đáp ứng nhu cầu của bạn với tư cách là người học và chương trình này sẽ tiếp tục được cung cấp trong tương lai.

|  |
| --- |
| **Individual course feedback**  After you complete the last graded assignment within an individual course, you might be asked to complete a survey. This survey will revisit questions from the previous survey and ask what you have learned up to that point in the program. Again, filling out this information is voluntary but extremely beneficial to the program and future learners. |

**Phản hồi khóa học cá nhân**

Sau khi bạn hoàn thành bài tập được chấm điểm cuối cùng trong một khóa học riêng lẻ, bạn có thể được yêu cầu hoàn thành một bản khảo sát. Cuộc khảo sát này sẽ xem lại các câu hỏi từ cuộc khảo sát trước đó và hỏi bạn đã học được gì cho đến thời điểm đó trong chương trình. Xin nhắc lại, việc điền thông tin này là tự nguyện nhưng cực kỳ có lợi cho chương trình và người học sau này.

|  |
| --- |
| **Certificate completion survey**  After you complete the last graded assignment in the final (eighth) course of the certificate program, you will be asked to complete a survey that revisits some earlier questions and asks what you have learned throughout the duration of the program. This survey also asks whether you would like to share your contact information with prospective employers. Filling out the survey and sharing your contact information with prospective employers is completely optional and will not affect your course experience, scores, or ability to receive a certificate or job offer in any way. |

**Khảo sát hoàn thành chứng chỉ**

Sau khi bạn hoàn thành bài tập được chấm điểm cuối cùng trong khóa học cuối cùng (thứ tám) của chương trình chứng chỉ, bạn sẽ được yêu cầu hoàn thành một bản khảo sát để xem lại một số câu hỏi trước đó và hỏi bạn đã học được gì trong suốt thời gian của chương trình. Cuộc khảo sát này cũng hỏi xem bạn có muốn chia sẻ thông tin liên hệ của mình với các nhà tuyển dụng tiềm năng hay không. Việc điền vào bản khảo sát và chia sẻ thông tin liên hệ của bạn với các nhà tuyển dụng tiềm năng là hoàn toàn tùy chọn và sẽ không ảnh hưởng đến kinh nghiệm, điểm số hoặc khả năng nhận chứng chỉ hoặc lời mời làm việc của bạn dưới bất kỳ hình thức nào.

## **Bản khảo sát dành cho người tham gia Chứng chỉ An ninh mạng của Google**

## **Kết nối với các bạn cùng lớp của bạn**

# **Giới thiệu về an ninh mạng**

## **Introduction to cybersecurity**

|  |
| --- |
| Imagine that you're preparing for a storm. You've received notification that a storm is coming. You prepare by gathering the tools and materials you'll need to stay safe. You make sure your windows and doors are secure. You assemble a first aid kit, tools, food and water. You're prepared. The storm hits and there are powerful winds and heavy rain. The storm is using its force to try and breach your home. You notice some water leaks and begin patching them quickly in order to minimize any risk or potential damage. |

Hãy tưởng tượng rằng bạn đang chuẩn bị cho một cơn bão. Bạn đã nhận được thông báo rằng một cơn bão đang đến. Bạn chuẩn bị bằng cách thu thập các công cụ và vật liệu cần thiết để giữ an toàn. Bạn đảm bảo cửa sổ và cửa ra vào của bạn được an toàn. Bạn tập hợp một bộ sơ cứu, dụng cụ, thực phẩm và nước uống. Bạn đã chuẩn bị sẵn sàng. Bão ập đến kèm theo gió mạnh và mưa lớn. Cơn bão đang sử dụng sức mạnh của nó để cố gắng xâm nhập vào nhà của bạn. Bạn nhận thấy một số rò rỉ nước và bắt đầu vá chúng nhanh chóng để giảm thiểu mọi rủi ro hoặc thiệt hại tiềm ẩn.

|  |
| --- |
| Handling a security incident is no different. Organizations must prepare for the storm by ensuring they have the tools to mitigate and quickly respond to outside threats. The objective is to minimize risk and potential damage. |

Xử lý một sự cố an ninh cũng không khác. Các tổ chức phải chuẩn bị cho cơn bão bằng cách đảm bảo họ có các công cụ để giảm thiểu và ứng phó nhanh chóng với các mối đe dọa bên ngoài. Mục tiêu là giảm thiểu rủi ro và thiệt hại có thể xảy ra.

|  |
| --- |
| As a security analyst, you'll work to protect your organization and the people it serves from a variety of risks and outside threats. And if a threat does get through, you and your team will provide a solution to remedy the situation. |

Với tư cách là nhà phân tích bảo mật, bạn sẽ làm việc để bảo vệ tổ chức của mình và những người mà tổ chức đó phục vụ khỏi nhiều rủi ro và mối đe dọa từ bên ngoài. Và nếu mối đe dọa vượt qua được, bạn và nhóm của bạn sẽ đưa ra giải pháp để khắc phục tình hình.

|  |
| --- |
| To help you better understand what this means, we'll define security and discuss the roles of security professionals in organizations. |

Để giúp bạn hiểu rõ hơn ý nghĩa của điều này, chúng tôi sẽ xác định bảo mật và thảo luận về vai trò của các chuyên gia bảo mật trong tổ chức.

|  |
| --- |
| Let's start with some definitions: Cybersecurity, or security, is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation. |

Hãy bắt đầu với một số định nghĩa: An ninh mạng hay bảo mật là hoạt động đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin bằng cách bảo vệ mạng, thiết bị, con người và dữ liệu khỏi bị truy cập trái phép hoặc khai thác trái phép.

|  |
| --- |
| For example, requiring complex passwords to access sites and services improves confidentiality by making it much more difficult for a threat actor to compromise them. A threat actor is any person or group who presents a security risk. |

Ví dụ: yêu cầu mật khẩu phức tạp để truy cập các trang web và dịch vụ sẽ cải thiện tính bảo mật bằng cách khiến tác nhân đe dọa khó xâm phạm chúng hơn nhiều. Tác nhân đe dọa là bất kỳ cá nhân hoặc nhóm nào có nguy cơ bảo mật.

|  |
| --- |
| Now that you know the definition of security, let's discuss what security teams do for an organization. |

Bây giờ bạn đã biết định nghĩa về bảo mật, hãy cùng thảo luận xem nhóm bảo mật sẽ làm gì cho một tổ chức.

|  |
| --- |
| Security protects against external and internal threats. An external threat is someone outside of the organization trying to gain access to private information, networks or devices. |

An ninh bảo vệ chống lại các mối đe dọa bên ngoài và bên trong. Mối đe dọa bên ngoài là ai đó bên ngoài tổ chức đang cố gắng truy cập vào thông tin, mạng hoặc thiết bị riêng tư.

|  |
| --- |
| An internal threat comes from current or former employees, external vendors, or trusted partners. Often these internal threats are accidental, such as an employee clicking on a compromised link in an email. Other times, the internal actor intentionally engages in activities such as unauthorized data access or abusing systems for personal use. |

Mối đe dọa nội bộ đến từ nhân viên hiện tại hoặc nhân viên cũ, nhà cung cấp bên ngoài hoặc đối tác đáng tin cậy. Thông thường, những mối đe dọa nội bộ này là vô tình, chẳng hạn như nhân viên nhấp vào liên kết bị xâm phạm trong email. Trong những trường hợp khác, tác nhân nội bộ cố tình tham gia vào các hoạt động như truy cập dữ liệu trái phép hoặc lạm dụng hệ thống để sử dụng cho mục đích cá nhân.

|  |
| --- |
| Experienced security professionals will help organizations mitigate or reduce the impact of threats like these. |

Các chuyên gia bảo mật có kinh nghiệm sẽ giúp các tổ chức giảm thiểu hoặc giảm thiểu tác động của các mối đe dọa như thế này.

|  |
| --- |
| Security teams also ensure an organization meets regulatory compliance, or laws and guidelines, that require the implementation of specific security standards. |

Các nhóm bảo mật cũng đảm bảo tổ chức đáp ứng việc tuân thủ quy định hoặc luật pháp và hướng dẫn yêu cầu triển khai các tiêu chuẩn bảo mật cụ thể.

|  |
| --- |
| Ensuring that organizations are in compliance may allow them to avoid fines and audits, while also upholding their ethical obligation to protect users. |

Việc đảm bảo rằng các tổ chức tuân thủ có thể cho phép họ tránh bị phạt tiền và kiểm tra, đồng thời duy trì nghĩa vụ đạo đức của mình để bảo vệ người dùng.

|  |
| --- |
| Security teams also maintain and improve business productivity. By establishing a plan for business continuity, security teams allow people to do their jobs, even in the case of something like a data breach. |

Điều chắc chắn rằng các tổ chức cộng thủ có thể cho phép họ tránh bị phạt tiền và kiểm tra, đồng thời duy trì nghĩa vụ đạo đức của mình để bảo vệ người sử dụng.

|  |
| --- |
| Being security conscious can also reduce expenses associated with risks, such as recovering from data loss or operational downtime, and potentially avoiding fines. The last benefit of security that we'll discuss is maintaining brand trust. If services or customer data are compromised, this can lower trust in the organization, damage the brand, and hurt the business in the long term. Loss of customer trust may also lead to less revenue for the business. |

Ý thức về bảo mật cũng có thể giảm chi phí liên quan đến rủi ro, chẳng hạn như khôi phục sau khi mất dữ liệu hoặc thời gian ngừng hoạt động và có khả năng tránh bị phạt. Lợi ích cuối cùng của bảo mật mà chúng ta sẽ thảo luận là duy trì niềm tin vào thương hiệu. Nếu dịch vụ hoặc dữ liệu khách hàng bị xâm phạm, điều này có thể làm giảm niềm tin vào tổ chức, làm tổn hại đến thương hiệu và gây tổn hại cho doanh nghiệp về lâu dài. Mất niềm tin của khách hàng cũng có thể dẫn đến doanh thu ít hơn cho doanh nghiệp.

|  |
| --- |
| Now, let's go over some common security-based roles. After completing this certificate program, here are some job titles you may want to search for: Security analyst or specialist, Cybersecurity analyst or specialist, Security operation center or SOC analyst, Information security analyst. |

Bây giờ, chúng ta hãy điểm qua một số vai trò dựa trên bảo mật phổ biến. Sau khi hoàn thành chương trình chứng chỉ này, dưới đây là một số chức danh công việc bạn có thể muốn tìm kiếm: Nhà phân tích hoặc chuyên gia bảo mật, nhà phân tích hoặc chuyên gia An ninh mạng, Trung tâm điều hành bảo mật hoặc nhà phân tích SOC, nhà phân tích bảo mật thông tin.

|  |
| --- |
| You'll also learn more about the responsibilities associated with some of these job titles later in the program. |

Bạn cũng sẽ tìm hiểu thêm về trách nhiệm liên quan đến một số chức danh công việc này ở phần sau của chương trình.

|  |
| --- |
| As you may now realize, the field of security includes many topics and concepts and every activity you complete in this program moves you one step closer to a new job. Let's keep learning together. |

Như bây giờ bạn có thể nhận ra, lĩnh vực bảo mật bao gồm nhiều chủ đề và khái niệm và mọi hoạt động bạn hoàn thành trong chương trình này sẽ đưa bạn đến gần hơn một bước với công việc mới. Hãy cùng nhau tiếp tục học tập nhé.

## **Toni: My path to cybersecurity**

|  |
| --- |
| Hi, I'm Toni, I'm a Security Engineering Manager. Our teams protect Google and its users from serious threats. Usually government-backed attackers, coordinated influence operations and serious cybercrime threat actors. I grew up as an army brat. My dad was in the military and we moved around a lot. I've always had an interest in security sort of generally. I got really hooked on international relations when I was in high school. I did a lot of Model United Nations. And that really sort of brought these two things together for me, the way that security works in the world. I come from a big family. I knew I was going to need financial assistance to go to college. And the Department of Defense provides a lot of educational opportunities that are tied to service. So this was a natural fit for me. I knew I was interested in this area and this was going to provide a career path into something I was passionate about. I started as an intelligence analyst, but not focused on cybersecurity. I worked counterinsurgency for a number of years and geopolitical intelligence issues. Eventually, as I looked and saw that the way that cybersecurity was starting to have an impact both in our daily lives and in that world of international relations, I got more and more drawn to it. Transitioning into cybersecurity was a huge shift for me. I came in without a solid technical background, had to learn a lot of that on the job and through self-paced learning in different types of courses, I needed to learn programming languages like Python and SQL, two of the things that we cover in this certificate, I needed to learn a whole new language about the vocabulary of threats and the different components and how those manifest technically. One of the things that I had to figure out very early in this journey is what kind of learner I was. I work best with a structured learning style. So turning to a lot of these online courses and resources that took this material and structured it sort of from first principles through application resonated very well for me. A lot of this was also learned on the job by co-workers who were willing to share and invest time in helping me understand this. I asked a lot of questions and I still do. Most of cybersecurity work is going to be learned on the job in the specific environment that you're protecting. So you have to work well with your teammates in order to be able to build that knowledge base. My advice would be to stay curious and keep learning, especially focusing on your technical skills and growing those throughout your career. It's really easy to get imposter syndrome in cybersecurity because it's so broad and mastery of all these different areas is a lifetime's work. And sometimes that imposter syndrome can shut us down and make it feel like, why bother trying to keep growing. I'm never going to be able to master this instead of motivating us. So keep learning, push through that fear. The efforts always going to be rewarded. |

Xin chào, tôi là Toni, tôi là Giám đốc Kỹ thuật Bảo mật. Nhóm của chúng tôi bảo vệ Google và người dùng của Google khỏi các mối đe dọa nghiêm trọng. Thường là những kẻ tấn công được chính phủ hậu thuẫn, các hoạt động gây ảnh hưởng phối hợp và các tác nhân đe dọa tội phạm mạng nghiêm trọng. Tôi lớn lên như một cậu nhóc quân đội. Bố tôi làm trong quân đội và chúng tôi di chuyển rất nhiều nơi. Nói chung, tôi luôn quan tâm đến vấn đề bảo mật. Tôi thực sự say mê quan hệ quốc tế khi còn học trung học. Tôi đã làm rất nhiều Mô hình Liên Hợp Quốc. Và điều đó thực sự đã mang hai thứ này lại với nhau đối với tôi, cách thức hoạt động của bảo mật trên thế giới. Tôi đên tư một gia đinh lơn. Tôi biết tôi sẽ cần hỗ trợ tài chính để đi học đại học. Và Bộ Quốc phòng cung cấp rất nhiều cơ hội giáo dục gắn liền với việc phục vụ. Vì vậy, đây là một sự phù hợp tự nhiên đối với tôi. Tôi biết tôi quan tâm đến lĩnh vực này và điều này sẽ mang lại con đường sự nghiệp cho lĩnh vực mà tôi đam mê. Tôi bắt đầu làm nhà phân tích tình báo, nhưng không tập trung vào an ninh mạng. Tôi đã làm việc trong lĩnh vực chống nổi dậy trong nhiều năm và nghiên cứu các vấn đề tình báo địa chính trị. Cuối cùng, khi tôi xem xét và nhận thấy rằng an ninh mạng bắt đầu có tác động đến cả cuộc sống hàng ngày của chúng ta và trong thế giới quan hệ quốc tế, tôi ngày càng bị cuốn hút vào nó. Chuyển sang lĩnh vực an ninh mạng là một sự thay đổi lớn đối với tôi. Tôi đến đây mà không có nền tảng kỹ thuật vững chắc, phải học rất nhiều thứ trong công việc và thông qua việc tự học theo các loại khóa học khác nhau, tôi cần học các ngôn ngữ lập trình như Python và SQL, hai trong số những thứ chúng tôi đề cập trong Chứng chỉ này, tôi cần học một ngôn ngữ hoàn toàn mới về từ vựng của các mối đe dọa và các thành phần khác nhau cũng như cách chúng biểu hiện về mặt kỹ thuật. Một trong những điều mà tôi phải nhận ra từ rất sớm trong cuộc hành trình này là tôi là loại người học tập như thế nào. Tôi làm việc hiệu quả nhất với phong cách học tập có cấu trúc. Vì vậy, việc chuyển sang sử dụng nhiều khóa học và tài nguyên trực tuyến sử dụng tài liệu này và cấu trúc nó từ những nguyên tắc đầu tiên cho đến ứng dụng đã tạo được tiếng vang rất lớn đối với tôi. Rất nhiều điều trong số này cũng đã được học hỏi trong công việc bởi những đồng nghiệp sẵn sàng chia sẻ và đầu tư thời gian để giúp tôi hiểu điều này. Tôi đã hỏi rất nhiều câu hỏi và tôi vẫn làm. Hầu hết công việc an ninh mạng sẽ được học trong công việc trong môi trường cụ thể mà bạn đang bảo vệ. Vì vậy, bạn phải phối hợp tốt với đồng đội của mình thì mới có thể xây dựng được nền tảng kiến ​​thức đó. Lời khuyên của tôi là hãy luôn tò mò và không ngừng học hỏi, đặc biệt là tập trung vào các kỹ năng kỹ thuật của bạn và phát triển chúng trong suốt sự nghiệp của bạn. Thực sự rất dễ mắc phải hội chứng kẻ mạo danh trong lĩnh vực an ninh mạng vì nó quá rộng và việc thành thạo tất cả các lĩnh vực khác nhau này là công việc cả đời. Và đôi khi hội chứng kẻ mạo danh đó có thể khiến chúng ta im lặng và khiến chúng ta cảm thấy như thế, tại sao phải cố gắng tiếp tục phát triển. Tôi sẽ không bao giờ có thể làm chủ được điều này thay vì động viên chúng tôi. Vì vậy, hãy tiếp tục học hỏi, vượt qua nỗi sợ hãi đó. Những nỗ lực luôn được đền đáp xứng đáng.

## **Responsibilities of an entry-level cybersecurity analyst**

|  |
| --- |
| Technology is rapidly changing and so are the tactics and techniques that attackers use. As digital infrastructure evolves, security professionals are expected to continually grow their skills in order to protect and secure sensitive information. In this video, we'll discuss some job responsibilities of an entry-level security analyst. |

Công nghệ đang thay đổi nhanh chóng và các chiến thuật cũng như kỹ thuật mà kẻ tấn công sử dụng cũng vậy. Khi cơ sở hạ tầng kỹ thuật số phát triển, các chuyên gia bảo mật dự kiến ​​sẽ liên tục phát triển kỹ năng của mình để bảo vệ và bảo mật thông tin nhạy cảm. Trong video này, chúng ta sẽ thảo luận về một số trách nhiệm công việc của một nhà phân tích bảo mật cấp mới vào nghề.

|  |
| --- |
| So, what do security analysts do? Security analysts are responsible for monitoring and protecting information and systems. |

Vậy, các nhà phân tích chứng khoán làm gì? Các nhà phân tích bảo mật chịu trách nhiệm giám sát và bảo vệ thông tin và hệ thống.

|  |
| --- |
| Now, we'll discuss three primary responsibilities of a security analyst, starting with protecting computer and network systems. Protecting computer and network systems requires an analyst to monitor an organization's internal network. If a threat is detected, then an analyst is generally the first to respond. Analysts also often take part in exercises to search for weaknesses in an organization's own systems. |

Bây giờ, chúng ta sẽ thảo luận ba trách nhiệm chính của một nhà phân tích bảo mật, bắt đầu bằng việc bảo vệ hệ thống mạng và máy tính. Bảo vệ hệ thống máy tính và mạng đòi hỏi nhà phân tích phải giám sát mạng nội bộ của tổ chức. Nếu một mối đe dọa được phát hiện thì nhà phân tích thường là người đầu tiên phản ứng. Các nhà phân tích cũng thường tham gia vào các hoạt động tìm kiếm điểm yếu trong hệ thống của tổ chức.

|  |
| --- |
| For example, a security analyst may contribute to penetration testing or ethical hacking. The goal is to penetrate or hack their own organization's internal network to identify vulnerabilities and suggest ways to strengthen their security measures. |

Ví dụ: một nhà phân tích bảo mật có thể đóng góp vào việc kiểm tra thâm nhập hoặc hack có đạo đức. Mục tiêu là xâm nhập hoặc hack mạng nội bộ của tổ chức họ để xác định các lỗ hổng và đề xuất cách tăng cường các biện pháp bảo mật của họ.

|  |
| --- |
| Think of it like this. After you lock your car, you check the door handles to make sure no one can access any valuables you keep inside. |

Hãy nghĩ về nó như thế này. Sau khi khóa xe, bạn kiểm tra tay nắm cửa để đảm bảo không ai có thể lấy được bất kỳ vật có giá trị nào bạn để bên trong.

|  |
| --- |
| Security analysts also proactively work to prevent threats from happening in the first place. One way they do this is by working with information technology, or IT, teams to install prevention software for the purposes of identifying risks and vulnerabilities. |

Các nhà phân tích bảo mật cũng chủ động làm việc để ngăn chặn các mối đe dọa xảy ra ngay từ đầu. Một cách để họ thực hiện điều này là làm việc với các nhóm công nghệ thông tin hoặc CNTT để cài đặt phần mềm phòng ngừa nhằm mục đích xác định rủi ro và lỗ hổng.

|  |
| --- |
| Analysts may also be involved in software and hardware development. They'll often work with development teams to support product security by setting up appropriate processes and systems to meet the organization's data protection needs. |

Các nhà phân tích cũng có thể tham gia phát triển phần mềm và phần cứng. Họ thường làm việc với các nhóm phát triển để hỗ trợ bảo mật sản phẩm bằng cách thiết lập các quy trình và hệ thống phù hợp nhằm đáp ứng nhu cầu bảo vệ dữ liệu của tổ chức.

|  |
| --- |
| The last task we'll discuss is conducting periodic security audits. A security audit is a review of an organization's security records, activities, and other related documents. For example, an analyst may examine in-house security issues, such as making sure that confidential information, like individual computer passwords, isn't available to all employees. |

Nhiệm vụ cuối cùng chúng ta sẽ thảo luận là tiến hành kiểm tra bảo mật định kỳ. Kiểm toán bảo mật là việc xem xét hồ sơ, hoạt động bảo mật và các tài liệu liên quan khác của tổ chức. Ví dụ: một nhà phân tích có thể kiểm tra các vấn đề bảo mật nội bộ, chẳng hạn như đảm bảo rằng thông tin bí mật, như mật khẩu máy tính cá nhân, không được cung cấp cho tất cả nhân viên.

|  |
| --- |
| Phew, that was a lot to cover! But hopefully you have a general idea of what entry-level security analysts do on a day-to-day basis. |

Phù, có quá nhiều thứ cần phải giải quyết! Nhưng hy vọng bạn có ý tưởng chung về công việc hàng ngày của các nhà phân tích bảo mật cấp thấp.

|  |
| --- |
| Security analysts are an important part of any organization. Their daily tasks protect small businesses, large companies, nonprofit organizations, and government agencies. They also help to ensure that the people served by those organizations remain safe. |

Các nhà phân tích bảo mật là một phần quan trọng của bất kỳ tổ chức nào. Nhiệm vụ hàng ngày của họ là bảo vệ các doanh nghiệp nhỏ, công ty lớn, tổ chức phi lợi nhuận và cơ quan chính phủ. Chúng cũng giúp đảm bảo rằng những người được các tổ chức đó phục vụ vẫn được an toàn.

## **Nikki: A day in the life of a security engineer**

|  |
| --- |
| [MUSIC] My name is Nikki and I'm a security engineer at Google. I am part of the insider threat detection team at Google, so my role is more focused on catching insider threats or insider suspicious activity within the company. My first experience with cybersecurity was when I was interning at the aquarium. I learned a lot of network security there, they had a lot of phishing attempts, of course, you know, at the aquarium. My manager was really focused on making sure that our networks were secure and I learned a lot from him and that really sparked my interest in cybersecurity. The main reason I chose to pursue a career in cybersecurity is just how flexible the career path is. Once you're in security, there's so many different fields you can dive into. Whether it's through the blue team, protecting the user or the red team, which is just, you know, poking holes in other people's defenses and letting them know where they're going wrong. A day in the life as a entry-level security professional? Um, it can change day to day, but there's two basic parts to it. There's the operation side, which is responding to detections and doing investigations. And then there's the project side where you're working with other teams to build new detections or improve the current detections. The difference between this entry-level cybersecurity analyst and an entry-level cybersecurity engineer is pretty much that the analyst is more focused on operations and the engineer, while they can do operations, they also build the, the detections and they do more project focused work. My favorite task is probably the operations side doing investigations because we can sometimes get something like this actor did such and such on this day. And we're supposed to then dive into what they've been doing, what they've been working on to figure out if there's any suspicious activity or if it was just a false positive. One of the biggest ways I've made an impact as an entry-level cybersecurity professional is actually working on the playbooks that, um, our team uses. A playbook is a list of how to go through a certain detection, and what the analyst needs to look at in order to investigate those incidents. I was really proud of those, those playbooks that I've made so far because a lot of my teammates have even said how helpful they've been to them. If you love solving problems, if you love protecting user data, being at the front lines of a lot of headlines, then this is definitely the role for you. |

[NHẠC] Tên tôi là Nikki và tôi là kỹ sư bảo mật tại Google. Tôi là thành viên của nhóm phát hiện mối đe dọa nội bộ tại Google, vì vậy vai trò của tôi tập trung hơn vào việc phát hiện các mối đe dọa nội bộ hoặc hoạt động đáng ngờ từ nội bộ trong công ty. Trải nghiệm đầu tiên của tôi về an ninh mạng là khi tôi đang thực tập tại thủy cung. Tôi đã học được rất nhiều điều về an ninh mạng ở đó, họ đã thực hiện rất nhiều nỗ lực lừa đảo, bạn biết đấy, ở thủy cung. Người quản lý của tôi thực sự tập trung vào việc đảm bảo mạng của chúng tôi được an toàn và tôi đã học được rất nhiều điều từ anh ấy và điều đó thực sự khơi dậy sự quan tâm của tôi đối với an ninh mạng. Lý do chính khiến tôi chọn theo đuổi nghề an ninh mạng là vì con đường sự nghiệp linh hoạt đến mức nào. Khi bạn đã ở trạng thái bảo mật, có rất nhiều lĩnh vực khác nhau mà bạn có thể tham gia. Cho dù đó là thông qua đội xanh, bảo vệ người dùng hay đội đỏ, bạn biết đấy, điều đó chỉ là chọc thủng hàng phòng ngự của người khác và cho họ biết họ đã sai ở đâu. Một ngày trong cuộc đời của một chuyên gia bảo mật cấp đầu vào? Ừm, nó có thể thay đổi hàng ngày, nhưng nó có hai phần cơ bản. Có phía hoạt động, đang ứng phó với các phát hiện và thực hiện điều tra. Và sau đó là phía dự án nơi bạn đang làm việc với các nhóm khác để xây dựng các phát hiện mới hoặc cải thiện các phát hiện hiện tại. Sự khác biệt giữa nhà phân tích an ninh mạng cấp độ đầu vào này và kỹ sư an ninh mạng cấp độ đầu vào khá nhiều là nhà phân tích tập trung hơn vào hoạt động và kỹ sư, trong khi họ có thể thực hiện các hoạt động, họ cũng xây dựng, phát hiện và họ tập trung vào dự án hơn công việc. Nhiệm vụ yêu thích của tôi có lẽ là bên điều hành thực hiện các cuộc điều tra vì đôi khi chúng tôi có thể nhận được điều gì đó giống như diễn viên này đã làm như vậy vào ngày này. Và sau đó chúng ta phải đi sâu vào những gì họ đang làm, những gì họ đang tiến hành để tìm hiểu xem có bất kỳ hoạt động đáng ngờ nào hay đó chỉ là một kết quả dương tính giả. Một trong những cách lớn nhất mà tôi đã tạo ra tác động với tư cách là một chuyên gia an ninh mạng cấp độ đầu vào là thực sự làm việc trên các cẩm nang mà nhóm chúng tôi sử dụng. Cẩm nang là danh sách cách thực hiện một phát hiện nhất định và những gì nhà phân tích cần xem xét để điều tra những sự cố đó. Tôi thực sự tự hào về những cuốn sách đó, những cuốn sách mà tôi đã làm cho đến nay bởi vì nhiều đồng đội của tôi thậm chí còn nói rằng chúng đã giúp ích cho họ như thế nào. Nếu bạn thích giải quyết vấn đề, nếu bạn thích bảo vệ dữ liệu người dùng, đứng đầu trên nhiều tiêu đề, thì đây chắc chắn là vai trò dành cho bạn.

## **Common cybersecurity terminology**

|  |
| --- |
| As you’ve learned, **cybersecurity** (also known as security) is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation. In this reading, you’ll be introduced to some key terms used in the cybersecurity profession. Then, you’ll be provided with a resource that’s useful for staying informed about changes to cybersecurity terminology. |

Như bạn đã biết, an ninh mạng (còn được gọi là bảo mật) là biện pháp đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin bằng cách bảo vệ mạng, thiết bị, con người và dữ liệu khỏi bị truy cập trái phép hoặc khai thác trái phép. Trong bài đọc này, bạn sẽ được giới thiệu một số thuật ngữ chính được sử dụng trong ngành an ninh mạng. Sau đó, bạn sẽ được cung cấp một nguồn tài nguyên hữu ích để luôn cập nhật thông tin về những thay đổi đối với thuật ngữ an ninh mạng.

|  |
| --- |
| **Key cybersecurity terms and concepts**  There are many terms and concepts that are important for security professionals to know. Being familiar with them can help you better identify the threats that can harm organizations and people alike. A security analyst or cybersecurity analyst focuses on monitoring networks for breaches. They also help develop strategies to secure an organization and research information technology (IT) security trends to remain alert and informed about potential threats. Additionally, an analyst works to prevent incidents. In order for analysts to effectively do these types of tasks, they need to develop knowledge of the following key concepts. |

**Các thuật ngữ và khái niệm an ninh mạng chính**

Có nhiều thuật ngữ và khái niệm quan trọng mà các chuyên gia bảo mật cần biết. Làm quen với chúng có thể giúp bạn xác định rõ hơn các mối đe dọa có thể gây hại cho tổ chức cũng như mọi người. Một nhà phân tích bảo mật hoặc nhà phân tích an ninh mạng tập trung vào việc giám sát các mạng để phát hiện các vi phạm. Họ cũng giúp phát triển các chiến lược để bảo mật tổ chức và nghiên cứu các xu hướng bảo mật công nghệ thông tin (IT) để luôn cảnh giác và được thông báo về các mối đe dọa tiềm ẩn. Ngoài ra, một nhà phân tích làm việc để ngăn ngừa sự cố. Để các nhà phân tích thực hiện hiệu quả các loại nhiệm vụ này, họ cần phát triển kiến ​​thức về các khái niệm chính sau.

|  |
| --- |
| **Compliance** is the process of adhering to internal standards and external regulations and enables organizations to avoid fines and security breaches. |

**Tuân thủ l**à quá trình tuân thủ các tiêu chuẩn nội bộ và quy định bên ngoài, đồng thời cho phép các tổ chức tránh bị phạt và vi phạm an ninh.

|  |
| --- |
| **Security frameworks** are guidelines used for building plans to help mitigate risks and threats to data and privacy. |

**Khung bảo mật** là các nguyên tắc được sử dụng để xây dựng kế hoạch nhằm giúp giảm thiểu rủi ro và mối đe dọa đối với dữ liệu và quyền riêng tư.

|  |
| --- |
| **Security controls** are safeguards designed to reduce specific security risks. They are used with security frameworks to establish a strong security posture. |

**Kiểm soát bảo mật** là các biện pháp bảo vệ được thiết kế để giảm thiểu rủi ro bảo mật cụ thể. Chúng được sử dụng cùng với các khung bảo mật để thiết lập một thế trận bảo mật mạnh mẽ.

|  |
| --- |
| **Security posture** is an organization’s ability to manage its defense of critical assets and data and react to change. A strong security posture leads to lower risk for the organization. |

**Tình trạng bảo mật** là khả năng của tổ chức trong việc quản lý việc bảo vệ các tài sản và dữ liệu quan trọng cũng như phản ứng với những thay đổi. Một trạng thái bảo mật mạnh mẽ dẫn đến rủi ro thấp hơn cho tổ chức.

|  |
| --- |
| A **threat actor**, or malicious attacker, is any person or group who presents a security risk. This risk can relate to computers, applications, networks, and data. |

**Tác nhân đe dọa** hoặc kẻ tấn công độc hại là bất kỳ cá nhân hoặc nhóm nào gây ra rủi ro bảo mật. Rủi ro này có thể liên quan đến máy tính, ứng dụng, mạng và dữ liệu.

|  |
| --- |
| An **internal threat** can be a current or former employee, an external vendor, or a trusted partner who poses a security risk. At times, an internal threat is accidental. For example, an employee who accidentally clicks on a malicious email link would be considered an accidental threat. Other times, the internal threat actor *intentionally* engages in risky activities, such as unauthorized data access. |

**Mối đe dọa nội bộ** có thể là nhân viên hiện tại hoặc nhân viên cũ, nhà cung cấp bên ngoài hoặc đối tác đáng tin cậy gây ra rủi ro bảo mật. Đôi khi, một mối đe dọa nội bộ là vô tình. Ví dụ: một nhân viên vô tình nhấp vào liên kết email độc hại sẽ bị coi là mối đe dọa vô tình. Đôi khi, tác nhân đe dọa nội bộ cố tình tham gia vào các hoạt động rủi ro, chẳng hạn như truy cập dữ liệu trái phép.

|  |
| --- |
| **Network security** is the practice of keeping an organization's network infrastructure secure from unauthorized access. This includes data, services, systems, and devices that are stored in an organization’s network. |

**An ninh mạng** là hoạt động giữ an toàn cho cơ sở hạ tầng mạng của một tổ chức khỏi bị truy cập trái phép. Điều này bao gồm dữ liệu, dịch vụ, hệ thống và thiết bị được lưu trữ trong mạng của tổ chức.

|  |
| --- |
| **Cloud security** is the process of ensuring that assets stored in the cloud are properly configured, or set up correctly, and access to those assets is limited to authorized users. The cloud is a network made up of a collection of servers or computers that store resources and data in remote physical locations known as data centers that can be accessed via the internet. Cloud security is a growing subfield of cybersecurity that specifically focuses on the protection of data, applications, and infrastructure in the cloud. |

**Bảo mật đám mây** là quá trình đảm bảo rằng các tài sản được lưu trữ trên đám mây được định cấu hình đúng cách hoặc được thiết lập chính xác và quyền truy cập vào các tài sản đó được giới hạn ở những người dùng được ủy quyền. Đám mây là một mạng được tạo thành từ một tập hợp các máy chủ hoặc máy tính lưu trữ tài nguyên và dữ liệu ở các vị trí vật lý từ xa được gọi là trung tâm dữ liệu có thể được truy cập qua internet. Bảo mật đám mây là một lĩnh vực an ninh mạng đang phát triển, đặc biệt tập trung vào việc bảo vệ dữ liệu, ứng dụng và cơ sở hạ tầng trên đám mây.

|  |
| --- |
| **Programming** is a process that can be used to create a specific set of instructions for a computer to execute tasks. These tasks can include:   * Automation of repetitive tasks (e.g., searching a list of malicious domains) * Reviewing web traffic * Alerting suspicious activity |

**Lập trình** là một quá trình có thể được sử dụng để tạo ra một bộ hướng dẫn cụ thể để máy tính thực hiện các tác vụ. Những nhiệm vụ này có thể bao gồm:

* Tự động hóa các tác vụ lặp đi lặp lại (ví dụ: tìm kiếm danh sách các miền độc hại)
* Xem xét lưu lượng truy cập web
* Cảnh báo hoạt động đáng ngờ

|  |
| --- |
| **Key takeaways**  Understanding key technical terms and concepts used in the security field will help prepare you for your role as a security analyst. Knowing these terms can help you identify common threats, risks, and vulnerabilities. To explore a variety of cybersecurity terms, visit the [National Institute of Standards and Technology glossary](https://csrc.nist.gov/glossary). Or use your browser to search for high-quality, reliable cybersecurity glossaries from research institutes or governmental authorities. Glossaries are available in multiple languages. |

**Bài học chính**

Hiểu các thuật ngữ và khái niệm kỹ thuật chính được sử dụng trong lĩnh vực bảo mật sẽ giúp bạn chuẩn bị cho vai trò là nhà phân tích bảo mật. Biết các thuật ngữ này có thể giúp bạn xác định các mối đe dọa, rủi ro và lỗ hổng phổ biến. Để khám phá nhiều thuật ngữ an ninh mạng, hãy truy cập bảng thuật ngữ của Viện Tiêu chuẩn và Công nghệ Quốc gia. Hoặc sử dụng trình duyệt của bạn để tìm kiếm các thuật ngữ an ninh mạng đáng tin cậy, chất lượng cao từ các viện nghiên cứu hoặc cơ quan chính phủ. Bảng thuật ngữ có sẵn bằng nhiều ngôn ngữ.

## **Test your knowledge: Introduction to cybersecurity**

# **Kỹ năng cốt lõi dành cho chuyên gia an ninh mạng**

## **Core skills for cybersecurity professionals**

|  |
| --- |
| **Core skills for cybersecurity professionals**  For any job, you need certain skills to be successful, and many of these core skills are transferable from one role to the next. No matter what job you currently have, you likely have many core skills already. Having a diverse background enhances your core skills, which means your personal experiences and perspectives are especially valuable. |

**Kỹ năng cốt lõi dành cho chuyên gia an ninh mạng**

Đối với bất kỳ công việc nào, bạn đều cần những kỹ năng nhất định để thành công và nhiều kỹ năng cốt lõi này có thể chuyển từ vai trò này sang vai trò tiếp theo. Cho dù hiện tại bạn đang làm công việc gì, bạn đều có thể đã có sẵn nhiều kỹ năng cốt lõi. Có nền tảng đa dạng sẽ nâng cao các kỹ năng cốt lõi của bạn, điều đó có nghĩa là kinh nghiệm và quan điểm cá nhân của bạn đặc biệt có giá trị.

|  |
| --- |
| In this video, we'll discuss both transferable and technical skills that are particularly useful for a security analyst. |

Trong video này, chúng ta sẽ thảo luận về cả kỹ năng chuyển giao và kỹ năng kỹ thuật đặc biệt hữu ích đối với nhà phân tích bảo mật.

|  |
| --- |
| Transferable skills are skills from other areas that can apply to different careers. |

Kỹ năng chuyển đổi là những kỹ năng từ các lĩnh vực khác có thể áp dụng cho các ngành nghề khác nhau.

|  |
| --- |
| Technical skills may apply to several professions as well. However, at times they may require knowledge of specific tools, procedures, and policies. |

Kỹ năng kỹ thuật cũng có thể áp dụng cho một số ngành nghề. Tuy nhiên, đôi khi họ có thể yêu cầu kiến ​​thức về các công cụ, thủ tục và chính sách cụ thể.

|  |
| --- |
| Let's discuss some core transferable skills you may already have that will benefit you in a career as a security analyst. Communication is a transferable skill for a security analyst. They will often need to describe certain threats, risks, or vulnerabilities to people who may not have a technical background. |

Hãy thảo luận về một số kỹ năng cốt lõi có thể chuyển giao mà bạn có thể đã có, điều này sẽ mang lại lợi ích cho bạn trong sự nghiệp phân tích chứng khoán. Giao tiếp là một kỹ năng có thể chuyển giao đối với một nhà phân tích bảo mật. Họ thường sẽ cần mô tả các mối đe dọa, rủi ro hoặc lỗ hổng nhất định cho những người có thể không có nền tảng kỹ thuật.

|  |
| --- |
| For example, security analysts may be tasked with interpreting and communicating policies and procedures to other employees. Or analysts may be asked to report findings to their supervisors, so the appropriate actions can be taken to secure the organization. |

Ví dụ, các nhà phân tích bảo mật có thể được giao nhiệm vụ giải thích và truyền đạt các chính sách và thủ tục cho các nhân viên khác. Hoặc các nhà phân tích có thể được yêu cầu báo cáo những phát hiện cho người giám sát của họ để có thể thực hiện các hành động thích hợp nhằm bảo đảm an toàn cho tổ chức.

|  |
| --- |
| Another transferable skill is collaboration. Security analysts often work in teams with engineers, digital forensic investigators, and program managers. For example, if you are working to roll out a new security feature, you will likely have a project manager, an engineer, and an ethical hacker on your team. Security analysts also need to be able to analyze complex scenarios that they may encounter. For example, a security analyst may need to make recommendations about how different tools can support efficiency and safeguard an organization's internal network. |

Một kỹ năng có thể chuyển giao khác là sự hợp tác. Các nhà phân tích bảo mật thường làm việc theo nhóm với các kỹ sư, nhà điều tra pháp y kỹ thuật số và người quản lý chương trình. Ví dụ: nếu bạn đang nỗ lực triển khai một tính năng bảo mật mới, bạn có thể sẽ có người quản lý dự án, kỹ sư và một hacker đạo đức trong nhóm của mình. Các nhà phân tích bảo mật cũng cần có khả năng phân tích các tình huống phức tạp mà họ có thể gặp phải. Ví dụ: nhà phân tích bảo mật có thể cần đưa ra khuyến nghị về cách các công cụ khác nhau có thể hỗ trợ hiệu quả và bảo vệ mạng nội bộ của tổ chức.

|  |
| --- |
| The last transferable skill that we'll discuss is problem-solving. Identifying a security problem and then diagnosing it and providing solutions is a necessary skill to keep business operations safe. Understanding threat actors and identifying trends can provide insight on how to handle future threats. |

Kỹ năng chuyển giao cuối cùng mà chúng ta sẽ thảo luận là giải quyết vấn đề. Xác định một vấn đề bảo mật, sau đó chẩn đoán nó và đưa ra giải pháp là một kỹ năng cần thiết để giữ cho hoạt động kinh doanh được an toàn. Hiểu các tác nhân đe dọa và xác định xu hướng có thể cung cấp cái nhìn sâu sắc về cách xử lý các mối đe dọa trong tương lai.

|  |
| --- |
| Okay, now that we've covered some important transferable skills, let's discuss some technical skills that security analysts need to develop. A basic understanding of programming languages is an important skill to develop because security analysts can use programming to automate tasks and identify error messages. |

Được rồi, bây giờ chúng ta đã đề cập đến một số kỹ năng chuyển giao quan trọng, hãy thảo luận về một số kỹ năng kỹ thuật mà các nhà phân tích bảo mật cần phát triển. Hiểu biết cơ bản về ngôn ngữ lập trình là một kỹ năng quan trọng cần phát triển vì các nhà phân tích bảo mật có thể sử dụng lập trình để tự động hóa các tác vụ và xác định các thông báo lỗi.

|  |
| --- |
| Like learning any other language, learning a programming language may seem challenging at first. However, this certificate program assumes no prior programming experience, so we'll start at the very beginning and provide several opportunities for hands-on practice with languages like Python and SQL. |

Giống như học bất kỳ ngôn ngữ nào khác, việc học một ngôn ngữ lập trình lúc đầu có vẻ khó khăn. Tuy nhiên, chương trình chứng chỉ này yêu cầu bạn không có kinh nghiệm lập trình trước đó, vì vậy chúng tôi sẽ bắt đầu ngay từ đầu và cung cấp một số cơ hội thực hành thực hành với các ngôn ngữ như Python và SQL.

|  |
| --- |
| Another important technical skill is knowing how to use security information and event management, or SIEM, tools. Security professionals use SIEM tools to identify and analyze security threats, risks, and vulnerabilities. For example, a SIEM tool may alert you that an unknown user has accessed the system. In the event of an unknown user accessing the system, you may use computer forensics to investigate the incident. |

Một kỹ năng kỹ thuật quan trọng khác là biết cách sử dụng các công cụ quản lý sự kiện và thông tin bảo mật hoặc SIEM. Các chuyên gia bảo mật sử dụng các công cụ SIEM để xác định và phân tích các mối đe dọa, rủi ro và lỗ hổng bảo mật. Ví dụ: công cụ SIEM có thể cảnh báo bạn rằng một người dùng không xác định đã truy cập hệ thống. Trong trường hợp người dùng không xác định truy cập vào hệ thống, bạn có thể sử dụng pháp y máy tính để điều tra vụ việc.

|  |
| --- |
| Now, let's discuss computer forensics. Similar to an investigator and a forensic scientist working in the criminal justice system, digital forensic investigators will attempt to identify, analyze, and preserve criminal evidence within networks, computers, and electronic devices. |

Bây giờ chúng ta hãy thảo luận về pháp y máy tính. Tương tự như điều tra viên và nhà khoa học pháp y làm việc trong hệ thống tư pháp hình sự, điều tra viên pháp y kỹ thuật số sẽ cố gắng xác định, phân tích và lưu giữ bằng chứng tội phạm trong mạng, máy tính và thiết bị điện tử.

|  |
| --- |
| Keep in mind that you may already have some of the core skills we've discussed. And if you don't have the technical skills, that's okay! This program is designed to support you in learning those skills. |

Hãy nhớ rằng bạn có thể đã có một số kỹ năng cốt lõi mà chúng ta đã thảo luận. Và nếu bạn không có kỹ năng kỹ thuật thì cũng không sao! Chương trình này được thiết kế để hỗ trợ bạn học những kỹ năng đó.

|  |
| --- |
| For example, over the past seven years working in cybersecurity, I've learned that security analysts need to have intellectual curiosity and the motivation to keep learning in order to succeed. Personally, I dedicate time on a regular basis towards learning more Python and SQL skills in order to meet the demands of the projects I'm working on. You'll get to learn about Python and SQL later in this program. |

Ví dụ, trong bảy năm làm việc trong lĩnh vực an ninh mạng, tôi đã học được rằng các nhà phân tích bảo mật cần phải có trí tò mò trí tuệ và động lực không ngừng học hỏi để thành công. Cá nhân tôi thường xuyên dành thời gian để học thêm các kỹ năng Python và SQL nhằm đáp ứng nhu cầu của các dự án mà tôi đang thực hiện. Bạn sẽ tìm hiểu về Python và SQL sau trong chương trình này.

|  |
| --- |
| As you continue this journey, you'll build the knowledge and skills you need to enter the security field. |

Khi tiếp tục hành trình này, bạn sẽ xây dựng kiến ​​thức và kỹ năng cần thiết để tham gia vào lĩnh vực bảo mật.

## **Veronica: My path to working in cybersecurity**

|  |
| --- |
| **Veronica: My path to working in cybersecurity**  Hi, I'm Veronica and I'm a security engineer at Google. My journey into cybersecurity has changed my life for the better in so many ways. The most important part is fulfilling work. I get to do something that I absolutely love and that I'm super interested in, and I feel very lucky that this is what I get to do for work. Before I entered my current field, I had no idea what cybersecurity was. My knowledge of cybersecurity was using secure passwords, and that was about it. So if you asked me, you know, would I be in cybersecurity five years ago? I would've said, what is that? Someone without a technical background can 100% be successful in cybersecurity. My path to my current role in cybersecurity started as an IT resident here at Google staff in Techstop. I learned a lot of analytical thinking skills, working on a help desk, troubleshooting, debugging. I didn't realize I had transferable skills until I got into my role in cybersecurity. And from there, I took it upon myself to bug a bunch of security engineers, interviewed a lot of them. I didn't get here alone. It took a village of mentors to get me here, so don't be afraid to ask for help. I don't think someone needs a college degree to go into cybersecurity. Some of the brightest minds that I get to work with don't have a college degree, so I think that's one of the best parts about the industry. Looking back at my career, I wish I would have known that I don't have to check all the boxes, that I don't have to be an expert in the area to shoot my shot, and I also wish I would've known that perfectionism can get in the way of what you want to achieve. |

**Veronica: Con đường làm việc trong lĩnh vực an ninh mạng của tôi**

Xin chào, tôi là Veronica và tôi là kỹ sư bảo mật tại Google. Hành trình của tôi vào lĩnh vực an ninh mạng đã thay đổi cuộc sống của tôi tốt hơn theo nhiều cách. Phần quan trọng nhất là hoàn thành công việc. Tôi được làm điều gì đó mà tôi thực sự yêu thích và cực kỳ hứng thú, đồng thời tôi cảm thấy rất may mắn vì đây là điều tôi được làm trong công việc. Trước khi bước vào lĩnh vực hiện tại, tôi không biết an ninh mạng là gì. Kiến thức của tôi về an ninh mạng là sử dụng mật khẩu an toàn và chỉ có vậy thôi. Vì vậy, nếu bạn hỏi tôi, bạn biết đấy, liệu tôi có tham gia lĩnh vực an ninh mạng 5 năm trước không? Tôi sẽ nói, đó là gì? Người không có nền tảng kỹ thuật có thể thành công 100% trong lĩnh vực an ninh mạng. Con đường dẫn đến vai trò hiện tại của tôi trong lĩnh vực an ninh mạng bắt đầu với tư cách là nhân viên CNTT tại nhân viên Google ở ​​Techstop. Tôi đã học được rất nhiều kỹ năng tư duy phân tích, làm việc trên bàn trợ giúp, xử lý sự cố, gỡ lỗi. Tôi đã không nhận ra mình có những kỹ năng có thể chuyển giao cho đến khi đảm nhận vai trò của mình trong lĩnh vực an ninh mạng. Và từ đó, tôi tự mình theo dõi một loạt kỹ sư bảo mật, phỏng vấn rất nhiều người trong số họ. Tôi không đến đây một mình. Phải mất cả làng cố vấn mới đưa được tôi đến đây, vì vậy đừng ngại yêu cầu giúp đỡ. Tôi không nghĩ ai đó cần có bằng đại học để theo học ngành an ninh mạng. Một số bộ óc thông minh nhất mà tôi được làm việc cùng không có bằng đại học, vì vậy tôi nghĩ đó là một trong những điểm hay nhất của ngành. Nhìn lại sự nghiệp của mình, tôi ước mình biết rằng tôi không cần phải đánh dấu vào tất cả các ô, rằng tôi không cần phải là chuyên gia trong lĩnh vực này mới có thể bắn được, và tôi cũng ước mình đã làm được điều đó. biết rằng chủ nghĩa hoàn hảo có thể cản trở những gì bạn muốn đạt được.

## **Transferable and technical cybersecurity skills**

|  |
| --- |
| **Transferable and technical cybersecurity skills**  Previously, you learned that cybersecurity analysts need to develop certain core skills to be successful at work. **Transferable skills** are skills from other areas of study or practice that can apply to different careers. **Technical skills** may apply to several professions, as well; however, they typically require knowledge of specific tools, procedures, and policies. In this reading, you’ll explore both transferable skills and technical skills further. |

**Kỹ năng an ninh mạng có thể chuyển giao và kỹ thuật**

Trước đây, bạn đã biết rằng các nhà phân tích an ninh mạng cần phát triển một số kỹ năng cốt lõi nhất định để thành công trong công việc. **Kỹ năng chuyển đổi** là những kỹ năng từ các lĩnh vực học tập hoặc thực hành khác có thể áp dụng cho các ngành nghề khác nhau. **Kỹ năng kỹ thuật** cũng có thể áp dụng cho một số ngành nghề; tuy nhiên, họ thường yêu cầu kiến ​​thức về các công cụ, thủ tục và chính sách cụ thể. Trong bài đọc này, bạn sẽ khám phá thêm cả kỹ năng chuyển giao và kỹ năng kỹ thuật.

|  |
| --- |
| **Transferable skills**  You have probably developed many transferable skills through life experiences; some of those skills will help you thrive as a cybersecurity professional. These include:   * **Communication:** As a cybersecurity analyst, you will need to communicate and collaborate with others. Understanding others’ questions or concerns and communicating information clearly to individuals with technical and non-technical knowledge will help you mitigate security issues quickly. * **Problem-solving:** One of your main tasks as a cybersecurity analyst will be to proactively identify and solve problems. You can do this by recognizing attack patterns, then determining the most efficient solution to minimize risk. Don't be afraid to take risks, and try new things. Also, understand that it's rare to find a perfect solution to a problem. You’ll likely need to compromise. * **Time management:** Having a heightened sense of urgency and prioritizing tasks appropriately is essential in the cybersecurity field. So, effective time management will help you minimize potential damage and risk to critical assets and data. Additionally, it will be important to prioritize tasks and stay focused on the most urgent issue. * **Growth mindset:** This is an evolving industry, so an important transferable skill is a willingness to learn. Technology moves fast, and that's a great thing! It doesn't mean you will need to learn it all, but it does mean that you’ll need to continue to learn throughout your career. Fortunately, you will be able to apply much of what you learn in this program to your ongoing professional development. * **Diverse perspectives:** The only way to go far is together. By having respect for each other and encouraging diverse perspectives and mutual respect, you’ll undoubtedly find multiple and better solutions to security problems. |

**Kỹ năng chuyển nhượng**

Bạn có thể đã phát triển nhiều kỹ năng có thể chuyển đổi thông qua kinh nghiệm sống; một số kỹ năng đó sẽ giúp bạn phát triển thành chuyên gia an ninh mạng. Bao gồm các:

* **Giao tiếp:** Là một nhà phân tích an ninh mạng, bạn sẽ cần giao tiếp và cộng tác với những người khác. Hiểu được câu hỏi hoặc mối quan tâm của người khác và truyền đạt thông tin rõ ràng đến những cá nhân có kiến ​​thức về kỹ thuật và phi kỹ thuật sẽ giúp bạn giảm thiểu các vấn đề bảo mật một cách nhanh chóng.
* **Giải quyết vấn đề:** Một trong những nhiệm vụ chính của bạn với tư cách là nhà phân tích an ninh mạng là chủ động xác định và giải quyết vấn đề. Bạn có thể làm điều này bằng cách nhận ra các kiểu tấn công, sau đó xác định giải pháp hiệu quả nhất để giảm thiểu rủi ro. Đừng ngại chấp nhận rủi ro và thử những điều mới. Ngoài ra, hãy hiểu rằng rất hiếm khi tìm được giải pháp hoàn hảo cho một vấn đề. Bạn có thể sẽ cần phải thỏa hiệp.
* **Quản lý thời gian:** Nâng cao ý thức cấp bách và sắp xếp thứ tự ưu tiên các nhiệm vụ một cách hợp lý là điều cần thiết trong lĩnh vực an ninh mạng. Vì vậy, quản lý thời gian hiệu quả sẽ giúp bạn giảm thiểu thiệt hại và rủi ro tiềm ẩn đối với các tài sản và dữ liệu quan trọng. Ngoài ra, điều quan trọng là phải ưu tiên các nhiệm vụ và tập trung vào vấn đề cấp bách nhất.
* **Tư duy phát triển:** Đây là một ngành đang phát triển, vì vậy một kỹ năng quan trọng có thể chuyển giao là sẵn sàng học hỏi. Công nghệ phát triển rất nhanh và đó là một điều tuyệt vời! Điều đó không có nghĩa là bạn sẽ cần phải học tất cả, nhưng điều đó có nghĩa là bạn sẽ cần phải tiếp tục học hỏi trong suốt sự nghiệp của mình. May mắn thay, bạn sẽ có thể áp dụng phần lớn những gì học được trong chương trình này vào quá trình phát triển nghề nghiệp đang diễn ra của mình.
* **Quan điểm đa dạng:** Con đường duy nhất để đi xa là cùng nhau. Bằng cách tôn trọng lẫn nhau và khuyến khích những quan điểm đa dạng cũng như tôn trọng lẫn nhau, chắc chắn bạn sẽ tìm thấy nhiều giải pháp tốt hơn và đa dạng hơn cho các vấn đề bảo mật.

|  |
| --- |
| **Technical skills**  There are many technical skills that will help you be successful in the cybersecurity field. You’ll learn and practice these skills as you progress through the certificate program. Some of the tools and concepts you’ll need to use and be able to understand include:   * **Programming languages:** By understanding how to use programming languages, cybersecurity analysts can automate tasks that would otherwise be very time consuming. Examples of tasks that programming can be used for include searching data to identify potential threats or organizing and analyzing information to identify patterns related to security issues. * **Security information and event management (SIEM) tools:** SIEM tools collect and analyze log data, or records of events such as unusual login behavior, and support analysts’ ability to monitor critical activities in an organization. This helps cybersecurity professionals identify and analyze potential security threats, risks, and vulnerabilities more efficiently. * **Intrusion detection systems (IDSs):** Cybersecurity analysts use IDSs to monitor system activity and alerts for possible intrusions. It’s important to become familiar with IDSs because they’re a key tool that every organization uses to protect assets and data. For example, you might use an IDS to monitor networks for signs of malicious activity, like unauthorized access to a network. * **Threat landscape knowledge:** Being aware of current trends related to threat actors, malware, or threat methodologies is vital. This knowledge allows security teams to build stronger defenses against threat actor tactics and techniques. By staying up to date on attack trends and patterns, security professionals are better able to recognize when new types of threats emerge such as a new ransomware variant. * **Incident response:** Cybersecurity analysts need to be able to follow established policies and procedures to respond to incidents appropriately. For example, a security analyst might receive an alert about a possible malware attack, then follow the organization’s outlined procedures to start the incident response process. This could involve conducting an investigation to identify the root issue and establishing ways to remediate it. |

**Kĩ năng công nghệ**

Có nhiều kỹ năng kỹ thuật sẽ giúp bạn thành công trong lĩnh vực an ninh mạng. Bạn sẽ học và thực hành những kỹ năng này khi bạn tiến bộ thông qua chương trình chứng chỉ. Một số công cụ và khái niệm bạn sẽ cần sử dụng và có thể hiểu được bao gồm:

* **Ngôn ngữ lập trình:** Bằng cách hiểu cách sử dụng ngôn ngữ lập trình, các nhà phân tích an ninh mạng có thể tự động hóa các tác vụ vốn rất tốn thời gian. Ví dụ về các tác vụ mà lập trình có thể được sử dụng bao gồm tìm kiếm dữ liệu để xác định các mối đe dọa tiềm ẩn hoặc tổ chức và phân tích thông tin để xác định các mẫu liên quan đến vấn đề bảo mật.
* **Công cụ quản lý sự kiện và thông tin bảo mật (SIEM):** Công cụ SIEM thu thập và phân tích dữ liệu nhật ký hoặc bản ghi các sự kiện như hành vi đăng nhập bất thường và hỗ trợ khả năng giám sát các hoạt động quan trọng trong tổ chức của nhà phân tích. Điều này giúp các chuyên gia an ninh mạng xác định và phân tích các mối đe dọa, rủi ro và lỗ hổng bảo mật tiềm ẩn hiệu quả hơn.
* **Hệ thống phát hiện xâm nhập (IDS):** Các nhà phân tích an ninh mạng sử dụng IDS để giám sát hoạt động của hệ thống và cảnh báo về các hành vi xâm nhập có thể xảy ra. Điều quan trọng là phải làm quen với IDS vì chúng là công cụ chính mà mọi tổ chức sử dụng để bảo vệ tài sản và dữ liệu. Ví dụ: bạn có thể sử dụng IDS để giám sát mạng nhằm phát hiện các dấu hiệu hoạt động độc hại, như truy cập trái phép vào mạng.
* **Kiến thức về bối cảnh mối đe dọa:** Nhận thức được các xu hướng hiện tại liên quan đến tác nhân đe dọa, phần mềm độc hại hoặc phương pháp đe dọa là rất quan trọng. Kiến thức này cho phép các nhóm bảo mật xây dựng hệ thống phòng thủ mạnh mẽ hơn trước các chiến thuật và kỹ thuật của tác nhân đe dọa. Bằng cách cập nhật các xu hướng và kiểu tấn công, các chuyên gia bảo mật có thể nhận biết tốt hơn khi các loại mối đe dọa mới xuất hiện, chẳng hạn như biến thể ransomware mới.
* **Ứng phó sự cố:** Các nhà phân tích an ninh mạng cần có khả năng tuân theo các chính sách và quy trình đã được thiết lập để ứng phó với sự cố một cách thích hợp. Ví dụ: nhà phân tích bảo mật có thể nhận được cảnh báo về một cuộc tấn công phần mềm độc hại có thể xảy ra, sau đó làm theo các quy trình được nêu ra của tổ chức để bắt đầu quá trình ứng phó sự cố. Điều này có thể liên quan đến việc tiến hành một cuộc điều tra để xác định vấn đề gốc rễ và thiết lập các cách để khắc phục nó.

|  |
| --- |
| **CompTIA Security+**  In addition to gaining skills that will help you succeed as a cybersecurity professional, the Google Cybersecurity Certificate helps prepare you for the [CompTIA Security+ exam](https://www.comptia.org/certifications/security), the industry leading certification for cybersecurity roles. You’ll earn a dual credential when you complete both, which can be shared with potential employers. After completing all eight courses in the Google Cybersecurity Certificate, you will unlock a 30% discount for the CompTIA Security+ exam and additional practice materials. |

**Bảo mật CompTIA+**

Ngoài việc đạt được các kỹ năng giúp bạn thành công với tư cách là chuyên gia an ninh mạng, Chứng chỉ an ninh mạng của Google còn giúp bạn chuẩn bị cho[Kỳ thi CompTIA Security+](https://www.comptia.org/certifications/security), chứng nhận hàng đầu trong ngành về vai trò an ninh mạng. Bạn sẽ nhận được chứng chỉ kép khi hoàn thành cả hai, chứng chỉ này có thể được chia sẻ với các nhà tuyển dụng tiềm năng. Sau khi hoàn thành tất cả tám khóa học trong Chứng chỉ an ninh mạng của Google, bạn sẽ được giảm giá 30% cho kỳ thi CompTIA Security+ và các tài liệu thực hành bổ sung.

|  |
| --- |
| **Key takeaways**  Understanding the benefits of core transferable and technical skills can help prepare you to successfully enter the cybersecurity workforce. Throughout this program, you’ll have multiple opportunities to develop these and other key cybersecurity analyst skills. |

**Bài học chính**

Hiểu được lợi ích của các kỹ năng kỹ thuật và chuyển giao cốt lõi có thể giúp bạn chuẩn bị gia nhập thành công lực lượng lao động an ninh mạng. Trong suốt chương trình này, bạn sẽ có nhiều cơ hội để phát triển những kỹ năng này và các kỹ năng phân tích an ninh mạng quan trọng khác.

## **Tầm quan trọng của an ninh mạng**

**The importance of cybersecurity**

|  |
| --- |
| As we've discussed security professionals protect many physical and digital assets. These skills are desired by organizations and government entities because risk needs to be managed. Let's continue to discuss why security matters. |

Như chúng ta đã thảo luận, các chuyên gia bảo mật bảo vệ nhiều tài sản vật lý và kỹ thuật số.Những kỹ năng này được các tổ chức mong muốn vàcác cơ quan chính phủ vì rủi ro cần phải được quản lý.Hãy tiếp tục thảo luận tại sao vấn đề bảo mật lại quan trọng.

|  |
| --- |
| Security is essential for ensuring an organization's business continuity and ethical standing. There are both legal implications and moral considerations to maintaining an organization's security. A data breach for example affects everyone that is associated with the organization. This is because data losses or leaks can affect an organization's reputation as well as the lives and reputations of their users clients and customers. By maintaining strong security measures  organizations can increase user trust. This may lead to financial growth and ongoing business referrals. |

Bảo mật là điều cần thiết để đảm bảo tính liên tục trong kinh doanh của tổ chức vàchỗ đứng đạo đức.Có cả ý nghĩa pháp lý vàcân nhắc về mặt đạo đức để duy trì an ninh của một tổ chức.Ví dụ, một vi phạm dữ liệuảnh hưởng đến tất cả những người có liên quan đến tổ chức.Điều này là do việc mất hoặc rò rỉ dữ liệu có thể ảnh hưởng đến danh tiếng của tổ chứccũng như tính mạng và danh tiếng của người sử dụng, khách hàng và khách hàng của họ.Bằng cách duy trì các biện pháp bảo mật mạnh mẽ, các tổ chức có thể tăng cường sự tin tưởng của người dùng.Điều này có thể dẫn đến tăng trưởng tài chính và giới thiệu kinh doanh liên tục.

|  |
| --- |
| As previously mentioned organizations are not the only ones that suffer during a data breach. Maintaining and securing user customer and vendor data is an important part of preventing incidents that may expose people's personally identifiable information. |

Như đã nói ở trên,các tổ chức không phải là những người duy nhất phải chịu thiệt hại khi vi phạm dữ liệu.Duy trì và bảo mật người dùng, khách hàng vàDữ liệu nhà cung cấp là một phần quan trọng trong việc ngăn chặn các sự cố có thể xảy ra.tiết lộ thông tin nhận dạng cá nhân của mọi người.

|  |
| --- |
| Personally identifiable information known as PII is any information used to infer an individual's identity. PII includes someone's full name date of birth physical address phone number email address internet protocol or IP address and similar information. |

Thông tin nhận dạng cá nhân, được gọi là PII, là bất kỳthông tin được sử dụng để suy ra danh tính của một cá nhân.PII bao gồm tên đầy đủ của ai đó, ngày sinh,địa chỉ vật lý, số điện thoại, địa chỉ email,giao thức internet hoặc địa chỉ IP và thông tin tương tự.

|  |
| --- |
| Sensitive personally identifiable information known as SPII is a specific type of PII that falls under stricter handling guidelines and may include social security numbers medical or financial information and biometric data such as facial recognition. If SPII is stolen this has the potential to be significantly more damaging to an individual than if PII is stolen. |

Thông tin nhận dạng cá nhân nhạy cảm, đã biếtdưới dạng SPII, là một loại PII cụ thể nằm trong các hướng dẫn xử lý chặt chẽ hơnvà có thể bao gồm số an sinh xã hội, y tế hoặcthông tin tài chính và dữ liệu sinh trắc học, chẳng hạn như nhận dạng khuôn mặt.Nếu SPII bị đánh cắp, điều này có khả năng gây thiệt hại đáng kể.gây tổn hại cho một cá nhân nhiều hơn nếu PII bị đánh cắp.

|  |
| --- |
| PII and SPII data are key assets that a threat actor will look for if an organization experiences a breach. When a person's identifiable information is compromised  leaked or stolen identity theft is the primary concern. |

Dữ liệu PII và SPII là tài sản chính mà kẻ đe dọa sẽ tìm kiếmnếu một tổ chức gặp phải vi phạm.Khi thông tin nhận dạng của một người bị xâm phạm, rò rỉ,hoặc bị đánh cắp, trộm cắp danh tính là mối quan tâm hàng đầu.

|  |
| --- |
| Identity theft is the act of stealing personal information to commit fraud while impersonating a victim. And the primary objective of identity theft is financial gain. |

Trộm cắp danh tính là hành vi đánh cắp thông tin cá nhân để thực hiện hành vi lừa đảotrong khi mạo danh nạn nhân.Và mục tiêu chính của hành vi trộm danh tính là thu lợi tài chính.

|  |
| --- |
| We've explored several reasons why security matters. Employers need security analysts like you to fill the current and future demand to protect data products and people while ensuring confidentiality integrity and safe access to information. This is why the U.S. Bureau of Labor Statistics expects the demand for security professionals to grow by more than 30% by the year 2030. |

Chúng tôi đã khám phá một số lý do tại sao vấn đề bảo mật lại quan trọng.Nhà tuyển dụng cần các nhà phân tích bảo mật như bạn để hoàn thành công việc hiện tại vànhu cầu trong tương lai để bảo vệ dữ liệu, sản phẩm và con người đồng thời đảm bảotính bảo mật, tính toàn vẹn và truy cập thông tin một cách an toàn.Đây là lý do tại sao Cục Thống kê Lao động Hoa Kỳ dự kiến ​​nhu cầu vềsố lượng chuyên gia bảo mật sẽ tăng hơn 30% vào năm 2030.

|  |
| --- |
| So keep learning and eventually you'll be able to do your part to create a safer and more secure environment for organizations and people alike! |

Vì vậy, hãy tiếp tục học hỏi và cuối cùng bạn sẽ có thể góp phần tạo ra một môi trường an toàn hơn vàmôi trường an toàn hơn cho các tổ chức và mọi người!​

## **Khám phá: Giữ an toàn cho tổ chức**

|  |
| --- |
| Learn to keep organizations secure |

Học cách giữ tổ chức chắc chắn

|  |  |
| --- | --- |
| Analytical thinking | Collaboration |
| A person in a wheelchair who is wearing a headset works at their desk on a computer. | Three people are gathered around a computer discussing an alert message on the screen. | |
| Analytical thinking  Security analysts often use **analytical thinking**, which means to think carefully and thoroughly. Analysts use this skill when **monitoring and securing computer and network systems**, responding to potential threats, defining system privileges, and determining ways to mitigate risk. | Collaboration  **Collaboration** means working with stakeholders and other team members. Security analysts often use this skill when **responding to an active threat.** They'll work with others when blocking unauthorized access and ensuring any compromised systems are restored. |

|  |  |
| --- | --- |
| Analytical thinking | Collaboration |
| **Tư duy phân tích**  Các nhà phân tích chứng khoán thường sử dụng tư duy phân tích, nghĩa là suy nghĩ cẩn thận và kỹ lưỡng. Các nhà phân tích sử dụng kỹ năng này khi giám sát và bảo mật hệ thống máy tính và mạng, ứng phó với các mối đe dọa tiềm ẩn, xác định đặc quyền hệ thống và xác định cách giảm thiểu rủi ro. | **Sự hợp tác**  Hợp tác có nghĩa là làm việc với các bên liên quan và các thành viên khác trong nhóm. Các nhà phân tích bảo mật thường sử dụng kỹ năng này khi ứng phó với một mối đe dọa đang diễn ra. Họ sẽ làm việc với những người khác khi chặn truy cập trái phép và đảm bảo mọi hệ thống bị xâm nhập đều được khôi phục. |

|  |  |
| --- | --- |
| Malware prevention | Communication |
| A person sits at a desk working on a computer. The screen shows that they have successfully installed prevention software. | A person gives a presentation in an office, discussing the security findings that are shown on a screen behind them. |
| Malware prevention  When a specific threat or vulnerability is identified, an analyst might **install prevention software**, which is software that works to proactively prevent a threat from occurring. Because malware is designed to harm devices or networks, **malware prevention** is essential. | Communication  As an analyst prevents and encounters threats, risks, or vulnerabilities, they document and **report findings.** A report might detail attempts to secure systems, test weak points, or offer solutions for system improvement. When reporting findings, strong **communication** skills are important. |

|  |  |
| --- | --- |
| Malware prevention | Communication |
| **Phòng chống phần mềm độc hại**  Khi xác định được một mối đe dọa hoặc lỗ hổng cụ thể, nhà phân tích có thể cài đặt phần mềm phòng ngừa, đây là phần mềm hoạt động để chủ động ngăn chặn mối đe dọa xảy ra. Vì phần mềm độc hại được thiết kế để gây hại cho thiết bị hoặc mạng nên việc ngăn chặn phần mềm độc hại là điều cần thiết. | **Giao tiếp**  Khi một nhà phân tích ngăn chặn và gặp phải các mối đe dọa, rủi ro hoặc lỗ hổng, họ sẽ ghi lại và báo cáo các phát hiện. Một báo cáo có thể trình bày chi tiết các nỗ lực nhằm bảo mật hệ thống, kiểm tra các điểm yếu hoặc đưa ra giải pháp cải tiến hệ thống. Khi báo cáo các phát hiện, kỹ năng giao tiếp tốt là rất quan trọng. |

|  |  |
| --- | --- |
| Understanding programming languages | Using SIEM tools |
| Two people are gathered in front of their computers, discussing code. | A person sits at a desk reviewing code on a tablet alongside other digital and physical documents that are on the desk. |
| Understanding programming languages  Analysts may sometimes work with software development teams to analyze and support security, install software, and set up appropriate processes. When involved with **software development** projects, it can be helpful for an analyst to **understand programming languages**. | Using SIEM tools  When security analysts need to review vulnerabilities, they conduct a **periodic security audit.** This is a review of an organization’s records, activities, and related documents. During audits, **Security Information and Event Management (SIEM) tools** help analysts better understand security threats, risks, and vulnerabilities. |

|  |  |
| --- | --- |
| Understanding programming languages | Using SIEM tools |
| **Hiểu ngôn ngữ lập trình**  Các nhà phân tích đôi khi có thể làm việc với các nhóm phát triển phần mềm để phân tích và hỗ trợ bảo mật, cài đặt phần mềm và thiết lập các quy trình thích hợp. Khi tham gia vào các dự án phát triển phần mềm, việc hiểu ngôn ngữ lập trình có thể hữu ích cho nhà phân tích. | **Sử dụng công cụ SIEM**  Khi các nhà phân tích bảo mật cần xem xét các lỗ hổng, họ sẽ tiến hành kiểm tra bảo mật định kỳ. Đây là việc xem xét hồ sơ, hoạt động và các tài liệu liên quan của tổ chức. Trong quá trình kiểm tra, các công cụ Quản lý sự kiện và thông tin bảo mật (SIEM) giúp các nhà phân tích hiểu rõ hơn về các mối đe dọa, rủi ro và lỗ hổng bảo mật. |

## **Giá trị của an ninh mạng**

## **Kiểm tra kiến ​​thức của bạn: Kỹ năng cốt lõi dành cho chuyên gia an ninh mạng**

# **Đánh giá: Chào mừng đến với thế giới đầy thú vị của An ninh mạng**

## **Gói lại**

|  |
| --- |
| **Wrap-up**  Congratulations on completing the first section of this course! Let's quickly review what we've covered so far, before moving on.  We defined security and introduced the benefits of implementing security in an organization. Then, we discussed different job responsibilities, such as managing threats and installing prevention software. We also introduced some important core skills, like collaboration and computer forensics. We finished by discussing the value of security and how it supports critical business functions.  I hope you've gained a greater understanding of security. If you feel like you need a refresher before moving on, you can always go back and review any content you're unsure about.  By learning the basics, you are laying the foundation for the rest of your security career.  Coming up, we'll explore some well-known attacks that shaped the security industry. I'm excited to continue this journey with you! |

**Gói lại**

Chúc mừng bạn đã hoàn thànhphần đầu tiên của khóa học này!Hãy nhanh chóng xem lại những gì chúng ta cóđược đề cập cho đến nay, trước khi tiếp tục.

Chúng tôi đã xác định bảo mật và giới thiệulợi ích của việc thực hiện bảo mật trong một tổ chức.Sau đó, chúng tôi thảo luận về các trách nhiệm công việc khác nhau,chẳng hạn như quản lý các mối đe dọavà cài đặt phần mềm phòng ngừa.Chúng tôi cũng giới thiệu một số kỹ năng cốt lõi quan trọng,như sự hợp tác và điều tra máy tính.Chúng ta kết thúc bằng việc thảo luận về giá trị của sự an toànvà cách nó hỗ trợ các chức năng kinh doanh quan trọng.

Tôi hy vọng bạn đã hiểu rõ hơn về bảo mật.Nếu bạn cảm thấy cần ôn lại trước khi tiếp tục,bạn luôn có thể quay lại và xem lạibất kỳ nội dung nào bạn không chắc chắn.

Bằng cách học những điều cơ bản,bạn đang đặt nền móng chophần còn lại của sự nghiệp bảo mật của bạn.

Sắp tới chúng ta sẽ khám phámột số cuộc tấn công nổi tiếng đã định hình ngành công nghiệp bảo mật.Tôi rất vui được tiếp tục cuộc hành trình này với bạn!

## **Thuật ngữ mô-đun 1**

|  |
| --- |
| **Glossary terms from module 1**  **Terms and definitions from Course 1, Module 1**  **Cybersecurity (or security):** The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation  **Cloud security:** The process of ensuring that assets stored in the cloud are properly configured and access to those assets is limited to authorized users  **Internal threat:** A current or former employee, external vendor, or trusted partner who poses a security risk  **Network security:** The practice of keeping an organization's network infrastructure secure from unauthorized access  **Personally identifiable information (PII):** Any information used to infer an individual’s identity  **Security posture:** An organization’s ability to manage its defense of critical assets and data and react to change  **Sensitive personally identifiable information (SPII):** A specific type of PII that falls under stricter handling guidelines  **Technical skills:** Skills that require knowledge of specific tools, procedures, and policies  **Threat:** Any circumstance or event that can negatively impact assets  **Threat actor:** Any person or group who presents a security risk  **Transferable skills:** Skills from other areas that can apply to different careers |

**Các thuật ngữ và định nghĩa trong Khóa 1, Học phần 1**

**An ninh mạng (hoặc bảo mật):** Thực tiễn đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin bằng cách bảo vệ mạng, thiết bị, con người và dữ liệu khỏi bị truy cập trái phép hoặc khai thác tội phạm

**Bảo mật đám mây:** Quá trình đảm bảo rằng các tài sản được lưu trữ trên đám mây được cấu hình đúng cách và quyền truy cập vào các tài sản đó được giới hạn ở những người dùng được ủy quyền

**Mối đe dọa nội bộ:** Nhân viên hiện tại hoặc cựu nhân viên, nhà cung cấp bên ngoài hoặc đối tác đáng tin cậy gây ra rủi ro bảo mật

**An ninh mạng:** Thực tiễn giữ an toàn cho cơ sở hạ tầng mạng của tổ chức khỏi bị truy cập trái phép

**Thông tin nhận dạng cá nhân (PII):** Bất kỳ thông tin nào được sử dụng để suy ra danh tính của một cá nhân

**Tình trạng bảo mật:** Khả năng của tổ chức trong việc quản lý việc bảo vệ các tài sản và dữ liệu quan trọng cũng như phản ứng với những thay đổi

**Thông tin nhận dạng cá nhân nhạy cảm (SPII):** Một loại PII cụ thể nằm trong các hướng dẫn xử lý chặt chẽ hơn

**Kỹ năng kỹ thuật:** Kỹ năng đòi hỏi kiến ​​thức về các công cụ, thủ tục và chính sách cụ thể

**Mối đe dọa:** Bất kỳ tình huống hoặc sự kiện nào có thể tác động tiêu cực đến tài sản

**Tác nhân đe dọa:** Bất kỳ cá nhân hoặc nhóm nào gây ra rủi ro bảo mật

**Kỹ năng có thể chuyển giao:** Kỹ năng từ các lĩnh vực khác có thể áp dụng cho các ngành nghề khác nhau

## **Thử thách mô-đun 1**